TOSHIBA

e-STUDIO550/650/810 用 スクランブラボード GP-1010

Security Target

TOEバージョン：V2.0

2004年02月25日

Ver 2.2

東芝テック株式会社

変更履歴

バージョン	変更日	変更内容	変更箇所	担当
1.0	2003/05/20	新規作成		木下/日永 佐々木
1.a	2003/06/10	・TOE範囲の一部見直しと明確化 ・セキュリティ機能名称，内容の見直し ・用語、略語の他証拠資料との表現統一 ・セキュリティ保証手段の証拠資料の明示	1-24,26-28, 30-33,36,37	木下/日永 佐々木
1.b	2003/07/01	・JEITA殿 ST ver 1.0に対する評価コメントの反映	1-10,16,17, 19-22,24-28, 30-34,36	木下/日永 佐々木
1.c	2003/08/28	・JEITA殿 ST ver 1.bに対する評価コメントの反映	1-8,10-25, 28-31,33-37, 39-41	木下/日永 佐々木
1.d	2003/09/04	・JEITA殿 ST ver 1.cに対する評価コメントの反映	1-6,8,9, 10-12,14-17, 19-24,26, 28-30,34-37, 40,41	木下/日永 佐々木
1.e	2003/10/07	・JEITA殿 ST ver 1.dに対する所見報告書ASE001-01～ASE005-01の内容反映 但し、ASE004-01の2.セキュリティ要件の相互作用(FPT_SEP.1)については未対応	1-6,8,9,12, 13,23-27, 29-30,32,33, 35-38,41-44	木下/日永 佐々木
1.f	2003/10/29	・JEITA殿 ST Ver 1.eに対する所見報告書ASE004-01の2.セキュリティ要件の相互作用(FPT_SEP.1)、及びASE006-01の内容反映	1-5,8,9,18, 23-24,26, 29-33,35-38, 42-46	木下/日永 佐々木
1.g	2003/11/08	・JEITA殿 ST Ver 1.fに対する所見報告書ASE007-01の内容反映、及び5.1.4の削除	1-8,11,14,17, 22,25-29,32, 34-35,38-39	木下/日永 佐々木
2.0	2004/02/05	・JEITA殿 ST Ver 1.gに対する所見報告書ASE008-01, ASE009-01, ASE010-01, ASE011-01, ASE012-01, ASE013-01, ASE014-01の内容反映、及びJEITA殿指摘事項反映と用語の統一	5,6,8,9,11,14, 18,22-25,28, 29,31,33-36, 39,41	木下/日永 佐々木
2.1	2004/02/17	・JEITA殿 ST Ver 2.0に対する所見報告書ASE015-02の内容反映	5,11,23, 25-29,33-36, 39	木下/日永 佐々木
2.2	2004/02/25	・JEITA殿 ST Ver 2.1に対する所見報告書ASE016-01の内容反映	5,6,22,23,29,33	木下/日永 佐々木

目次

1 ST概説

本章では、ST識別，ST概要，CC適合について記述する。また、本ST内で使用している用語や略語、及び商標について記述する。

1.1 ST識別

本STの識別情報は、以下の通りである。

ST名称　:e-STUDIO 550/650/810用スクランブラボード GP-1010 Security Target
STバージョン　:Ver 2.2
ST作成日　:2004年02月25日
ST作成者　:東芝テック株式会社 画像情報通信カンパニー
　東芝ソリューション株式会社
TOE名称　:e-STUDIO 550/650/810用スクランブラボード GP-1010
TOEバージョン　:V2.0
TOE製作者　:東芝テック株式会社 画像情報通信カンパニー
評価保証レベル　:EAL2
キーワード　:デジタル複写機，e-STUDIO，スクランブラボード，GP-1010，ハードディスク暗号化，東芝テック
CCのバージョン　:JIS X 5070-1:2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部:総則及び一般モデル
　JIS X 5070-2:2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部:セキュリティ機能要件
　JIS X 5070-3:2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部:セキュリティ保証要件
　CCIMB Interpretations-0210

尚、日本語訳は、以下のものを使用している。

- 「情報技術セキュリティ評価のためのコモンクライテリア パート1～パート3」平成13年1月翻訳 第1.2版
  情報処理振興事業協会(IPA) セキュリティセンター発行
- 「補足-0210」
  独立行政法人 製品評価技術基盤機構(NITE) 適合性評価センター発行

1.2 ST概要

本STは、東芝テック株式会社製 デジタル複写機「e-STUDIO 550/650/810」用の「スクランブラボード GP-1010」のセキュリティ仕様を定めたセキュリティターゲットである。
「e-STUDIO 550/650/810」は、一般的なオフィス等に設置されるデジタル複写機で、紙のドキュメント情報を電子的なイメージデータに変換することで、オフィス業務を電子的に支援する製品である。
「スクランブラボード GP-1010」は、「e-STUDIO 550/650/810」にオプションで実装され、電子的なイメージデータをHDDに書込み及び読出しを行う際のイメージデータの暗号化及び復号と、HDDの実データ領域の全消去を行う製品である。

1.3 CC適合

本STは、以下のCCに適合している。

- 機能要件は、JIS X 5070 第2部適合である。
- 保証要件は、JIS X 5070 第3部適合である。
- 評価保証レベルは、EAL2適合である。
- 本STが適合しているPPはない。

1.4 用語、略語

本STで使用している用語、略語は以下のものである。

CC関連の略語

- CC(Common Criteria):コモンクライテリア
- EAL(Evaluation Assurance Level):評価保証レベル
- PP(Protection Profile):プロテクションプロファイル
- ST(Security Target):セキュリティターゲット
- TOE(Target Of Evaluation):評価対象
- SFP(Security Function Policy):セキュリティ機能ポリシー
- SOF(Strength Of Function):機能強度
- TSF(TOE Security Functions):TOEセキュリティ機能
- TSP(TOE Security Policy):TOEセキュリティポリシー
- TSC(TSF Scope of Control):TOEセキュリティ機能制御範囲

TOE関連の用語、略語

- HDD (Hard Disk Drive)
  e-STUDIO 550/650/810に実装されているハードディスク装置。
- FAT(File Allocation Table)情報
  ハードディスク装置に格納されているファイルの管理領域の情報。
- Flash ROM
  システムボード上に実装されているROMで、e-STUDIO 550/650/810本体、及びスクランブラボードGP-1010を制御するためのソフトウェアがインストールされている不揮発性メモリ。
- NVRAM (NonVolatile RAM)
  システムボード上に実装されているRAMで、e-STUDIO 550/650/810の各種設定情報を格納する不揮発性メモリ。設定情報の一部にスクランブラボードの装着有無情報が含まれる。
- 拡張NVRAM
  システムボード上に実装されているRAMで、e-STUDIO 550/650/810の各種設定情報を格納する揮発性メモリ。設定情報の一部に暗号鍵データが含まれ、リチウムコイン電池により設定情報が保持されている。
- RTC（Real Time clock）
  システムボード上に実装されているICで、実時間に準じた時間データを発生する内部時計。
- KEY PLD (KEY Programable Logic Device)
  スクランブラボード上に実装されている論理素子で、e-STUDIO550/650/810起動時にシステムボード上の拡張NVRAMからスクランブラボード上に転送される暗号鍵データを保存する揮発性の論理素子(チップ)。
- FF値
  HDDデータ全消去機能のHDDへの書込みのデータ値で、8ビットの全ての値がオール"1"の状態を16進法であらわした値。
- BSP（Board Support Package）
  e-STUDIO550/650/810のシステムボードに依存するデバイスの初期設定処理などをパッケージ化したソフトウェア。
- TOEの関係者
  e-STUDIO利用者、及びe-STUDIO管理者，サービスエンジニア，e-STUDIO非関係者。
- ユーザ
  e-STUDIO 550/650/810の複写機能などの一般機能を利用するお客様を指す。具体的には、e-STUDIO利用者。
- ユーザ文書
  ユーザが扱う機密情報などの重要文書を含む文書。
- ROMデータ
  e-STUDIO550/650/810用の制御ソフトウェアで、Flash ROMに格納されるデータ。
- UIデータ
  タッチパネル上に表示される操作メッセージや表示アイコンなどに使用する各国語向けの言語データ。
- 鍵コード
  e-STUDIO管理者に提供される封筒に記載されたアルファベット(A～F)と数字(0～9)から成る暗号鍵のコード。
- 暗号鍵データ
  e-STUDIO管理者により入力された鍵コードが変換され、電子的に保存されている128bitのデータ。
  暗号化/復号操作で使用される暗号鍵は、パリティビットが除かれて112bitとなる。
- 暗号鍵作成会社
  FIPS140-2の統計的乱数性の検定に適合したセキュアであることが保証された暗号鍵を作成する会社であり、鍵コードとしてメーカに提供される。
- サービスマンコール表示
  e-STUDIO 550/650/810の障害や故障、セキュリティ侵害の可能性検出時において、サービスエンジニア呼び出しの旨を示すメッセージ表示のこと。
- スクランブラボード
  暗号化/復号操作を司るハードウェア(基板)単体を指す。
- スクランブラボード GP-1010
  TOE。暗号化/復号操作を司るハードウェアとHDDデータ全消去機能を含む関連するソフトウェアを指す。
- EPROM（Erasable Programmable ROM）
  紫外線により消去可能なROMで、システムボードのソフトウェアまたはUIデータを書込み、ダウンロード治具に装着して用いる。
- e-STUDIOアプリケーション
  複写機能やファイリング機能を利用した時に動作するソフトウェア群。

- e-STUDIO利用者機能
  デジタル複写機における、複写機能(コピー)、及びファイリング機能。
- 解読装置
  HDD内のデータを読み出し、解読する装置。

1.5 商標

- VxWorksは、Wind River Systems,Inc.の登録商標または商標です。
- 本STに記載の製品名称は、それぞれ各社が商標として使用している場合があります。

2 TOE記述

本章では、TOEの概要，TOEの関係者，物理的構成，論理的構成，保護資産、及びTOEの機能について記述する。

2.1 TOEの概要

2.1.1 TOE種別

TOEは、「e-STUDIO 550/650/810」という紙のドキュメント情報を電子的なイメージデータに変換する製品において、「スクランブラボード GP-1010」という、イメージデータをHDDに書込み及び読出しを行う際にイメージデータの暗号化及び復号を行うイメージデータ暗号化ボードと、HDDの実データ領域の全消去を行うソフトウェアから成る製品である。

2.1.2 利用目的

「スクランブラボード GP-1010」は、「e-STUDIO 550/650/810」においてHDDに格納される電子的なイメージデータを暗号化することと、「e-STUDIO 550/650/810」のHDDを廃棄または交換する際にデータ領域に残存しているデータを全消去することを目的としている。

2.1.3 主な機能

「e-STUDIO 550/650/810」はデジタル複写機であり、利用者の機能として以下のe-STUDIO利用者機能を提供する。

＜e-STUDIO利用者機能＞

- 複写機能(コピー)
  ボタン操作により、紙のユーザ文書情報がスキャナエンジンを介して、電子的なイメージデータに変換され、HDDに一時的に書込まれる。HDDに書込まれたイメージデータは、印刷用の画像データに変換され、ページメモリに一時的に書込まれる。プリンタエンジンは、ページメモリの画像データより紙への複写を行う。複写完了にて、HDD上に書込まれたイメージデータのFAT情報は消去される。
- ファイリング機能
  操作パネルにより、紙のユーザ文書情報がスキャナエンジンを介して、電子的なイメージデータに変換され、HDDに保存される。HDDに保存可能な文書数は24文書であり、操作パネルからの印刷操作により、HDDに保存されているイメージデータは、印刷用の画像データに変換され、ページメモリに一時的に書込まれる。プリンタエンジンは、ページメモリの画像データより、紙への複写を行う。操作パネルから消去操作を行ったときに、HDDに保存されているイメージデータのFAT情報は消去される。

「スクランブラボード GP-1010」は、「e-STUDIO 550/650/810」のe-STUDIO利用者機能である複写機能とファイリング機能にて、HDDに書込まれるユーザ文書のイメージデータの暗号化を行う。また、HDDの実データ領域に残存しているイメージデータを全消去する機能を提供する。

2.2 TOEの関係者

2.2.1 TOEの正規の関係者

本TOEにおける正規の関係者は、以下のものである。正規の関係者の役割、信頼度、知識について以下に記述する。

- e-STUDIO利用者
  役割　:「e-STUDIO 550/650/810」における複写等、デジタル複写機の一般的な機能を利用する。
  信頼度:信頼度は必ずしも高いとは言えない。他人の秘密文書を暴露しようとする、悪意を持った利用者がいる可能性がある。
  知識　:高度な情報処理技術を持たない。
- e-STUDIO管理者
  役割　:「e-STUDIO 550/650/810」に関する運用管理を行う。
  TOEに関しては、以下の役割を担う。
    - 「スクランブラボードGP-1010」導入時に、インストール作業を行うサービスエンジニアが、メーカまたはその関連会社や販売会社の社員であることを確認する。
    - 「スクランブラボードGP-1010」導入時のインストール作業において、サービスエンジニアからの依頼により、鍵コードが記載された封筒を開封して、それに記載されている鍵コードの入力を行う。鍵コード入力後は、その封筒を厳重に管理する。
    - 「e-STUDIO 550/650/810」本体を廃棄または交換する前に、サービスエンジニアにその旨を連絡し、HDDデータ全消去の依頼を行う。

  信頼度:「e-STUDIO 550/650/810」の利用部門の責任者より、e-STUDIO管理者として任命された者であり、信頼度は高い。TOEに対して、悪意をもった行為は行わない。
  知識　:「e-STUDIO 550/650/810」の利用、及びその運用管理に関する知識を有する。
- サービスエンジニア
  役割　:「e-STUDIO 550/650/810」の設置場所(オンサイト)において、「e-STUDIO 550/650/810」の設置，インストール，及び保守業務を行う。
  TOEに関しては、以下の役割を担う。
    - スクランブラボード GP-1010のインストールとして、スクランブラボードの装着，ソフトウェアのインストール，鍵コード入力後のHDDの初期化操作などの作業を行う。

- e-STUDIO管理者からの依頼により、e-STUDIO 550/650/810の廃棄または交換時にHDDデータ全消去の作業を行う。

  信頼度:「e-STUDIO 550/650/810」のメーカ、またはその関連会社、販売会社の社員であり、信頼度は高い。TOEに対して悪意をもった行為は行わない。
  知識　:「e-STUDIO 550/650/810」に関する保守技術に精通している。ITや情報処理技術については特に限定はしない。

2.2.2 TOEの正規でない関係者

本TOEにおける正規でない関係者は以下のものである。正規でない関係者の役割、信頼度、知識について以下に記述する。

- e-STUDIO非関係者
  役割　:特定の役割はなく、「e-STUDIO 550/650/810」に物理的にアクセス可能な人。
  信頼度:他人の秘密文書を暴露しようとする、悪意を持った第三者がいる可能性がある。
  知識　:高度な情報処理技術を持たない。

2.3 物理的構成

TOEを構成するハードウェアとソフトウェアの範囲を以下に示す。

2.3.1 ハードウェア構成

図2.3-1に、「スクランブラボード GP-1010」を実装した「e-STUDIO 550/650/810」のハードウェア構成を示す。
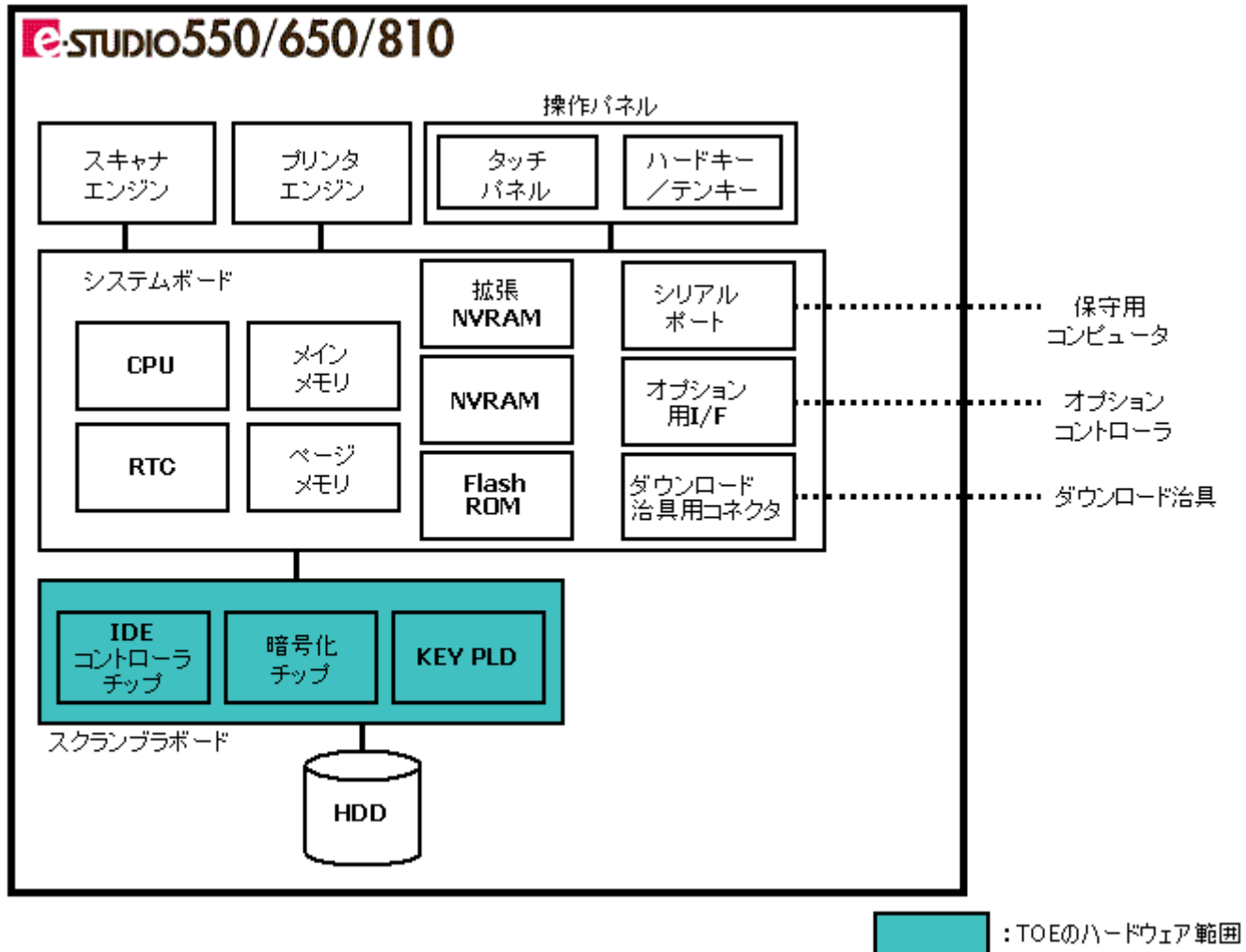
図2.3-1 「スクランブラボード GP-1010」装着時の「e-STUDIO 550/650/810」ハードウェア構成

＊ 本TOEのソフトウェアは、システムボード上のFlash ROMに格納される。

2.3.2 ハードウェア構成要素

ハードウェア構成における構成要素を以下に示す。

ハードウェア	仕様
スキャナエンジン	両面原稿対応 自動原稿送り装置
プリンタエンジン	レーザー静電転写方式 連続複写速度(A4横):55枚/分, 65枚/分, 81枚/分
操作パネル	・タッチパネル 　タッチパネル付グラフィック液晶ディスプレイ 　表示ドット数:320×240(1/4 VGA) ・ハードキー／テンキー 　複写機能における複写操作を行うキー(ボタン) 　テンキーは0から9までの数字キー(ボタン)
システムボード	【CPU】:システムの制御を行うための中央演算処理装置。TMPR3927/133MHz 【メインメモリ】:起動時にFlash ROMからシステムプログラムなどがロードされ、実行時のメモリとして使用される。サイズ:32MB 【ページメモリ】:原稿読取り時や印刷時に使用するメモリ。サイズ:32MB 【NVRAM】:e-STUDIO 550/650/810の各種設定情報を格納する不揮発性メモリ。設定情報の一部にスクランブラボードの装着有無情報や各種パラメータが含まれる。サイズ:8KB 【拡張NVRAM】:e-STUDIO 550/650/810の各種設定情報を格納するリチウムコイン電池により電源バックアップされている揮発性メモリ。設定情報の一部に暗号鍵データが含まれる。サイズ:128KB 　尚、拡張NVRAMとリチウムコイン電池は、それぞれシステムボードにハンダ付けされており、リチウムコイン電池から電源を供給したままの状態で取り外すことはできない。それらのどちらかを取り外した場合は、拡張NVRAMに電源が供給されなくなり、保持していた暗号鍵データは消去される。 　また、拡張NVRAMに格納されている暗号鍵データを解析するには、システムボードにデータ解析用の特殊な装置を取り付ける必要があり、低レベルの攻撃者が行なうことは不可能である。 【Flash ROM】:e-STUDIO 550/650/810本体、及びスクランブラボードGP-1010を制御するためのソフトウェアがインストールされている不揮発性メモリ。サイズ:4MB 【RTC】:実時間に準じた時間データを発生するIC。
スクランブラボード	部品名:PWA-F-DES-340 【IDEコントローラチップ】:HDDへのデータ転送を制御する論理素子(チップ)であり、スクランブラボードの装着確認用の識別情報を保持している。 【KEY PLD】:e-STUDIO550/650/810起動時にシステムボード上の拡張NVRAMからスクランブラボード上に転送される暗号鍵データを保存する揮発性の論理素子(チップ)。 【暗号化チップ】:HDDに書込むデータを暗号化し、HDDから読出すデータを復号するチップ。
HDD	内蔵3.5インチIDEハードディスク
シリアルポート	サービスエンジニアの保守情報収集用インタフェース。 サービスエンジニアが保守情報収集のための専用ソフトウェアを搭載した保守用コンピュータを接続する場合に使用する。 モデムや一般のコンピュータを接続して保守情報を収集することは不可能である。
オプション用I/F	e-STUDIO 550/650/810をネットワークプリンタ装置やネットワークスキャナ装置としてネットワークを介して使用する際に、接続するオプションコントローラ用のインタフェース。 e-STUDIO 550/650/810をネットワーク接続するには、オプション機器であるオプションコントローラを追加接続する必要があり、本TOEの構成では、ネットワークには接続できない。
ダウンロード治具用コネクタ	サービスエンジニアのプログラム及びUIデータダウンロード用の治具用コネクタ サービスエンジニアが、システムボードのソフトウェアまたはUIデータが書込まれているEPROMをダウンロード治具(基板)上に装着し、ダウンロード治具用コネクタに接続して、それぞれスクランブラボードGP-1010のソフトウェアはシステムボード上のFlash ROM, UIデータはHDDにダウンロードする。

2.3.3 ハードウェアのTOE範囲

ハードウェアのTOE範囲は、以下のものである。

- スクランブラボード
    - IDEコントローラチップ
    - KEY PLD
    - 暗号化チップ

2.3.4 ソフトウェア構成

図2.3-2に、「スクランブラボード GP-1010」を実装した「e-STUDIO 550/650/810」のソフトウェア構成を示す。
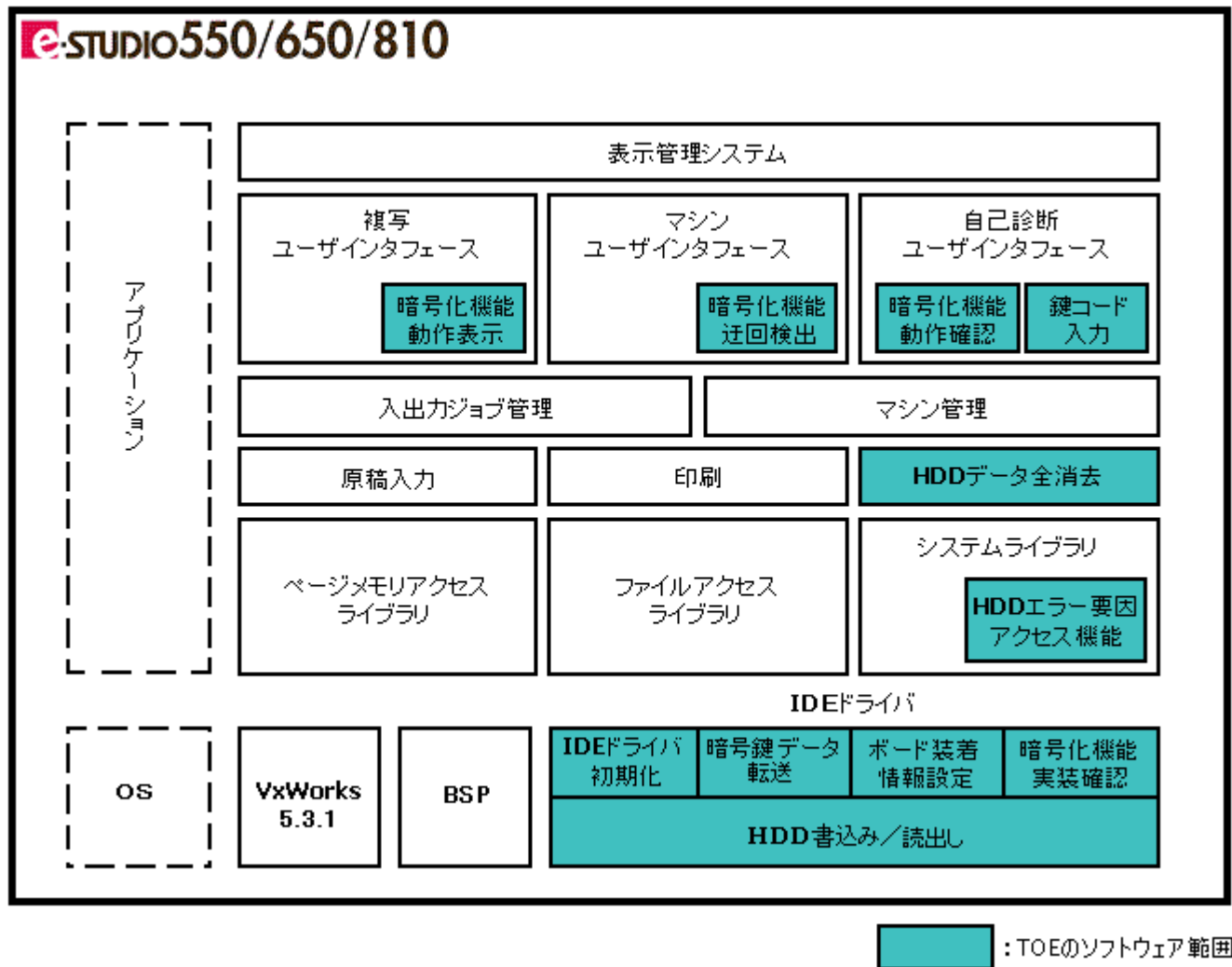
図2.3-2 「スクランブラボード GP-1010」装着時の「e-STUDIO 550/650/810」ソフトウェア構成

2.3.5 ソフトウェア構成要素

ソフトウェア構成における構成要素を以下に示す。

ソフトウェア	機能
表示管理システム	操作パネルにおけるタッチスクリーンの制御ドライバ。操作パネルで操作画面の表示とタッチスクリーン操作の入力座標データの受け取りを行う。入力座標のデータから、対象機能のユーザインタフェースプログラムへの実行指示を行う。
自己診断ユーザインタフェース	サービスエンジニア用の保守用ユーザインタフェース。保守用の情報確認のための自己診断機能の画面制御を行う。また、鍵コードの入力やスクランブラボードの実装有無の表示、HDDデータ全消去機能の実行指示を行う。 【暗号化機能動作確認】：スクランブラボードの装着有無情報をNVRAMから読出す要求を行う。 【鍵コード入力】：入力された鍵コードを、暗号鍵データとして拡張NVRAMへの書込みを行う。
マシンユーザインタフェース	「e-STUDIO 550/650/810」の状態を操作パネルに表示する。 【暗号化機能迂回検出】：暗号化機能実装確認により設定されたHDDエラー要因情報を取り出し、エラーが検出された時、操作パネルにサービスマンコール表示を行う。
複写ユーザインタフェース	複写機能画面の表示制御を行う。 【暗号化機能動作表示】：暗号化機能正常動作時にTOEのバージョン表示を行う。
入出力ジョブ管理	複写機能やファイリング機能の操作において、ユーザ文書原稿の読取り指示や紙への印刷、HDDへのファイルの格納や読出し等のジョブ全般の管理を行う。
マシン管理	「e-STUDIO 550/650/810」のマシン状態の管理を行う。

原稿入力	紙のユーザ文書原稿を、電子的なイメージデータに変換するための光学的な読取り制御を行う。
印刷	原稿入力により、読込んだ電子的なイメージデータに対して、印刷用のデータ変換処理を行い、紙への印刷を行う。
HDDデータ全消去	自己診断ユーザインタフェースからの実行要求により、HDDの実データ領域をデータ上書きにより消去する。消去の進捗状況を自己診断ユーザインタフェースに通知する。
システムライブラリ	「e-STUDIO 550/650/810」のマシン制御及びマシン情報の取得を行う 【HDDエラー要因アクセス機能】:暗号化機能実装確認時のHDDエラー要因情報へのアクセスを行う。
ファイルアクセスライブラリ	HDD内のファイルに対する生成、変更、削除などのアクセス要求を行う。
ページメモリアクセスライブラリ	ページメモリへの入出力制御を行う。
BSP (ボードサポートパッケージ)	Board Support Packageの略でe-STUDIO550/650/810のシステムボードに依存する処理をパッケージ化したソフトウェア。
IDEドライバ	【HDD書込み/読出し】:HDDへの全ての書込み/読出し処理を行う。 【IDEドライバ初期化】:IDEドライバの初期化を行う。 【暗号鍵データ転送】:システムボード上の拡張NVRAM から暗号鍵データを取り出し、スクランブラボード上のKEY PLDに暗号鍵データの転送を行う。 【ボード装着情報設定】:システムボード上のNVRAMにスクランブラボードの装着有無情報の設定を行う。 【暗号化機能実装確認】:スクランブラボードの装着状態の確認を行う。
VxWorks 5.3.1	オペレーティングシステム

2.3.6 ソフトウェアのTOE範囲

ソフトウェアのTOE範囲は、以下のものである。

- **暗号化機能動作表示** V 1.c
- **暗号化機能迂回検出** V 1.a
- **暗号化機能動作確認** V 1.b
- **鍵コード入力** V 1.b
- **HDDデータ全消去** V 1.a
- **HDDエラー要因アクセス機能** V 1.a
- **IDEドライバ** V 1.c
  - **HDD書込み/読出し**
  - **IDEドライバ初期化**
  - **暗号鍵データ転送**
  - **ボード装着情報設定**
  - **暗号化機能実装確認**

2.4 論理的構成

2.4.1 論理構成

図2.4-1に、「スクランブラボード GP-1010」を実装した「e-STUDIO 550/650/810」の論理構成とそのTOE範囲を示す。
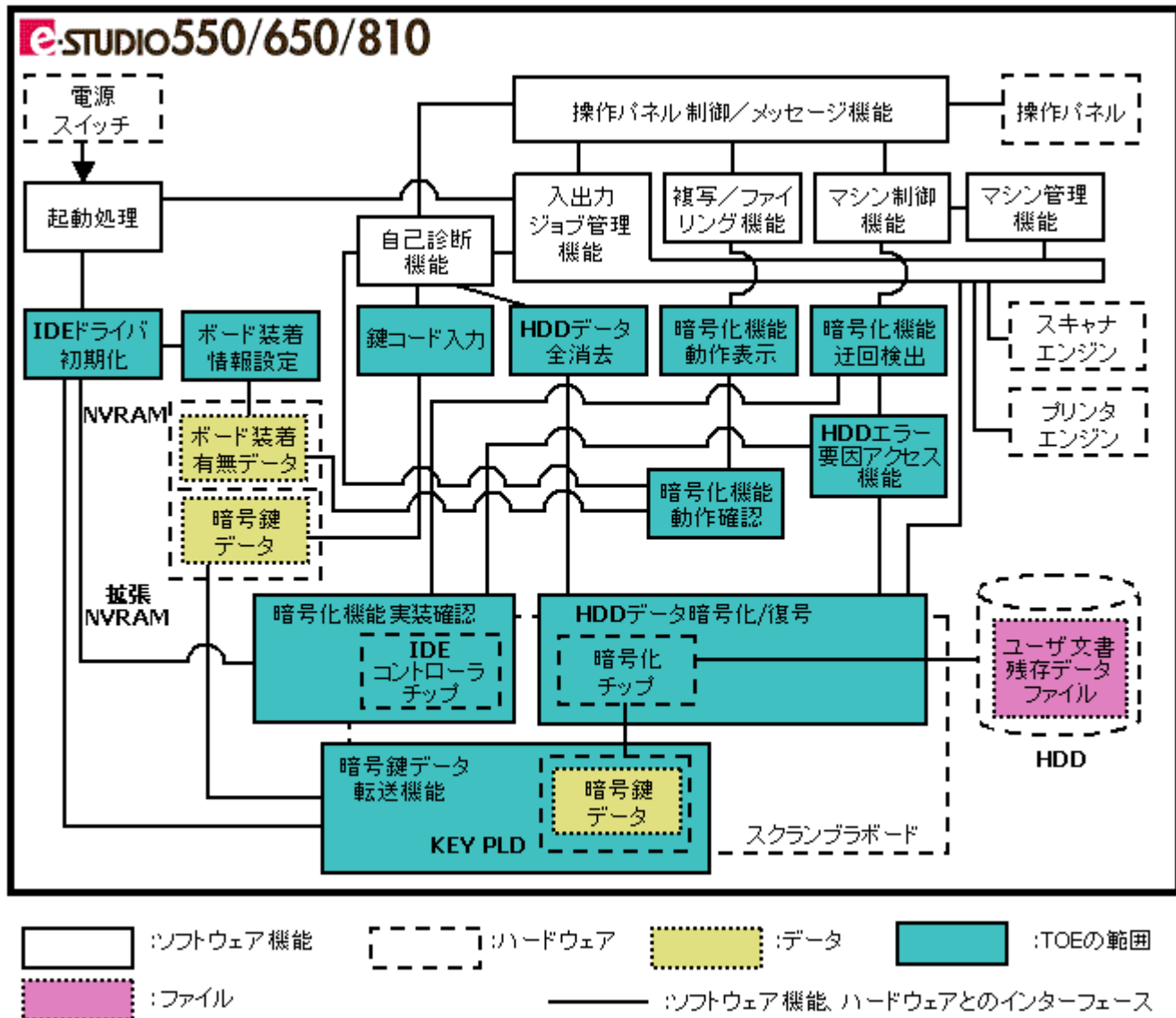
図2.4-1「e-STUDIO 550/650/810」論理構成

2.4.2 論理構成要素

論理構成における機能とハードウェア/ソフトウェア構成要素対応は、以下のものである。

・セキュリティ機能

機能名称	ハードウェア/ソフトウェア構成要素対応づけ
暗号化機能実装確認	S/W:暗号化機能実装確認(IDEドライバ) H/W:IDEコントローラチップ
HDDデータ全消去	S/W:HDDデータ全消去
暗号化機能動作表示	S/W:暗号化機能動作表示(複写ユーザインタフェース)
暗号化機能迂回検出	S/W:暗号化機能迂回検出(マシンユーザインタフェース)
HDDデータ暗号化／復号	S/W:HDD書込み/読出し(IDEドライバ) H/W:暗号化チップ

・非セキュリティ機能

機能名称	ハードウェア/ソフトウェア構成要素対応づけ
IDEドライバ初期化	S/W:IDEドライバ初期化(IDEドライバ)
暗号鍵データ転送	S/W:暗号鍵データ転送(IDEドライバ) H/W:KEY PLD
ボード装着情報設定	S/W:ボード装着情報設定(IDEドライバ)
鍵コード入力	S/W:鍵コード入力(自己診断ユーザインタフェース)
暗号化機能動作確認	S/W:暗号化機能動作確認(自己診断ユーザインタフェース)
HDDエラー要因アクセス機能	S/W:HDDエラー要因アクセス機能(システムライブラリ)
e-STUDIO起動処理	S/W:BSP
操作パネル制御／メッセージ機能	S/W:表示管理システム
自己診断機能	S/W:自己診断ユーザインタフェース
複写／ファイリング機能	S/W:複写ユーザインタフェース
マシン制御機能	S/W:マシンユーザインタフェース
マシン管理機能	S/W:マシン管理
入出力ジョブ管理機能	S/W:入出力ジョブ管理

2.4.3 論理構成のTOE範囲

論理構成のTOE範囲は、以下のものである。

- IDEドライバ初期化
- 暗号化機能実装確認
- 暗号鍵データ転送
- ボード装着情報設定
- 鍵コード入力
- HDDデータ全消去
- 暗号化機能動作表示
- 暗号化機能動作確認
- 暗号化機能迂回検出
- HDDエラー要因アクセス機能
- HDDデータ暗号化／復号

2.5 保護資産

本TOEの保護資産は、ユーザ文書残存データである。ユーザ文書残存データは、以下のものである。

- ユーザ文書残存データ

図2.5-1 に示すように、e-STUDIO利用者が複写機能を利用した際にユーザ文書の電子的なイメージデータファイルが生成されHDDに保存される。このイメージデータファイルは、複写完了のタイミングにてHDD上のFAT情報が消去されるが、実データ領域上にユーザ文書のイメージデータが残存する。
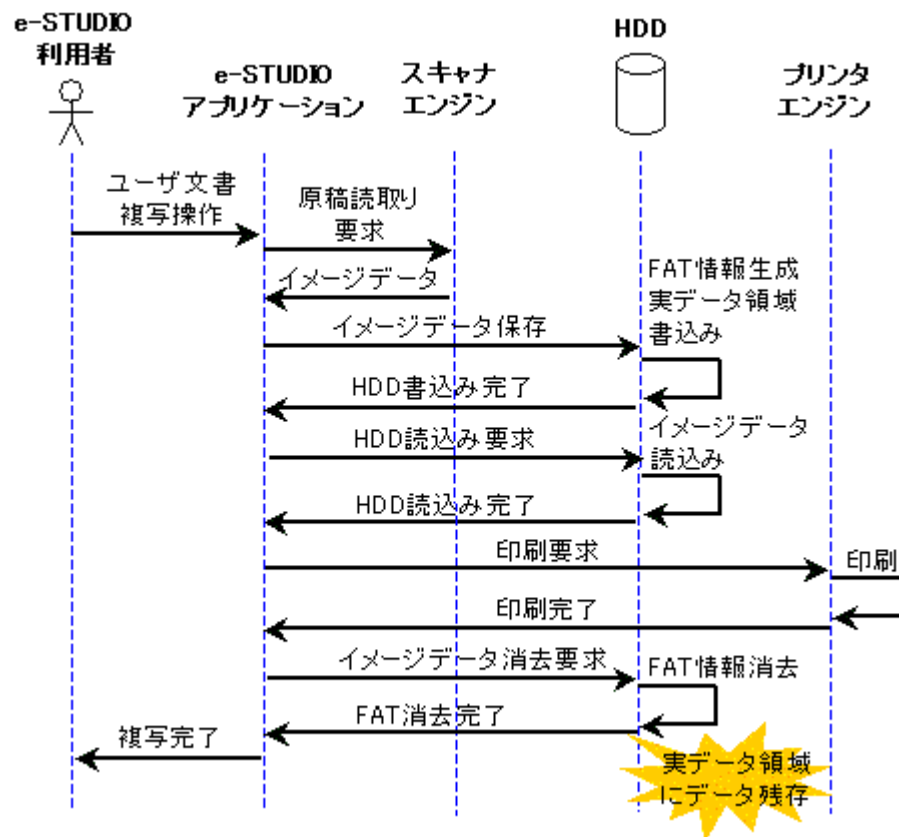
図2.5-1 複写機能利用時の処理の流れ

図2.5-2 に示すように、e-STUDIO利用者は、ファイリング機能を使用してユーザ文書の電子的なイメージデータファイルをHDDに登録しておき、自由に印刷することができる。このイメージデータファイルは、ファイリング機能の登録文書の消去操作のタイミングにてHDD上のFAT情報が消去されるが、実データ領域上にユーザ文書のイメージデータが残存する。
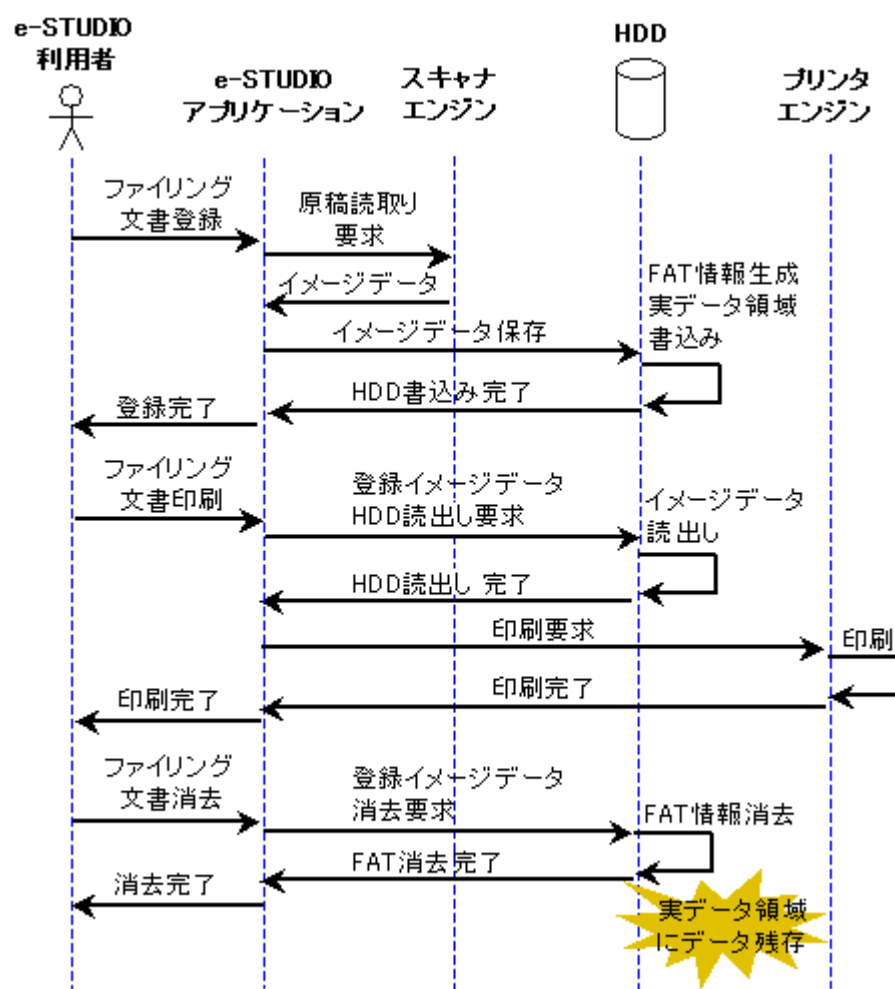
図2.5-2 ファイリング機能利用時の処理の流れ

以上、e-STUDIO利用者が複写機能やファイリング機能を利用した際に、複写完了、及びファイリング文書の消去操作時点でHDD上の実データ領域に残存するイメージデータをユーザ文書残存データと定義し、保護資産とする。

2.6 TOEの機能

2.6.1 TOEが提供する機能

本TOEが提供する機能は、以下のものである。

＜セキュリティ機能＞

- HDDデータ暗号化／復号機能
  e-STUDIO利用者が複写機能やファイリング機能を利用する時に、読込んだ紙のドキュメント情報を電子的なイメージデータに変換する際に暗号化してHDDに保存する。紙への印刷処理時にHDDに暗号化されて保存されているイメージデータを読出して復号する。
- HDDデータ全消去機能
  「e-STUDIO 550/650/810」のHDD廃棄または交換時に、HDDの実データ領域の全てのデータを上書き消去する。本機能は、サービスエンジニア向けの機能であり、e-STUDIO管理者からの依頼により実施される。
- 暗号化機能迂回検出機能
  スクランブラボードの装着状態の確認結果が異常であれば、操作パネル上にサービスエンジニアの呼出しを要求するサービスマンコール表示を行い、「e-STUDIO 550/650/810」の機能利用を停止する。
- 暗号化機能実装確認機能
  「e-STUDIO 550/650/810」の起動時に、スクランブラボードの装着状態の確認を行う。
- 暗号化機能動作表示機能
  暗号化機能が正常に動作しているとき、操作パネルからの表示要求により、TOEバージョンの表示を行う。

＜非セキュリティ機能＞

- 暗号化機能動作確認機能
  NVRAMに設定されているスクランブラボードの装着有無情報を取得する。
- IDEドライバ初期化機能
  e-STUDIO 550/650/810の起動時に、スクランブラボード装着状態の確認を行い、スクランブラボードの装着状態の確認結果が正常であれば、スクランブラボード上の拡張NVRAMから暗号鍵データを取り出し、スクランブラボード上のKEY PLDに暗号鍵データの転送を行う。
- 鍵コード入力機能
  TOEのインストール機能であり、スクランブラボード装着後にサービスエンジニアによって起動され、e-STUDIO管理者が操作パネルからアルファベット(A～F)と数字(0～9)からなる、暗号鍵作成会社が提供するFIPS140-2の統計的乱数性の検定に適合したセキュアな鍵コードの入力を行い、鍵コードの入力内容が正しければ、128bitの暗号鍵データに変換してシステムボードの拡張NVRAMに格納する。
- HDDエラー要因アクセス機能
  スクランブラボード装着確認で異常の場合、HDDエラー要因情報の取得を行う。
- 暗号鍵データ転送機能
  システムボードの拡張NVRAMから暗号鍵データを取り出し、スクランブラボード上のKEY PLDに暗号鍵データの転送を行う。
- ボード装着情報設定機能
  スクランブラボードの装着有無の情報をシステムボードのNVRAMに設定する。

2.6.2 TOEが提供しない機能

暗号鍵は暗号鍵作成会社が作成し、鍵コードとしてメーカに提供されるものであり、FIPS140-2の統計的乱数性の検定に適合したセキュアであることが保証された暗号鍵である。鍵コードは本TOEのインストール時に、サービスエンジニアよりe-STUDIO管理者に、TOEと一緒に提供される。e-STUDIO管理者が鍵コードをTOEに入力後、128bitの暗号鍵データに変換され、保存される。一度保存された暗号鍵データは、継続して使用することから、暗号鍵を生成、及び暗号鍵を破棄する必要はない。よって、以下の機能は提供しない。

- 暗号鍵生成機能
- 暗号鍵破棄機能

2.6.3 運用手順

TOEにおける以下の作業あるいは操作の運用は、e-STUDIO管理者とサービスエンジニアによって行われる。

- スクランブラボードGP-1010導入時
  - スクランブラボードの装着、ソフトウェア更新、鍵コード入力、UIデータのインストール、及びHDDの初期化
- e-STUDIO 550/650/810廃棄または交換時
  - HDDデータ全消去

図2.6-1にスクランブラボードGP-1010導入時の作業手順を示す。
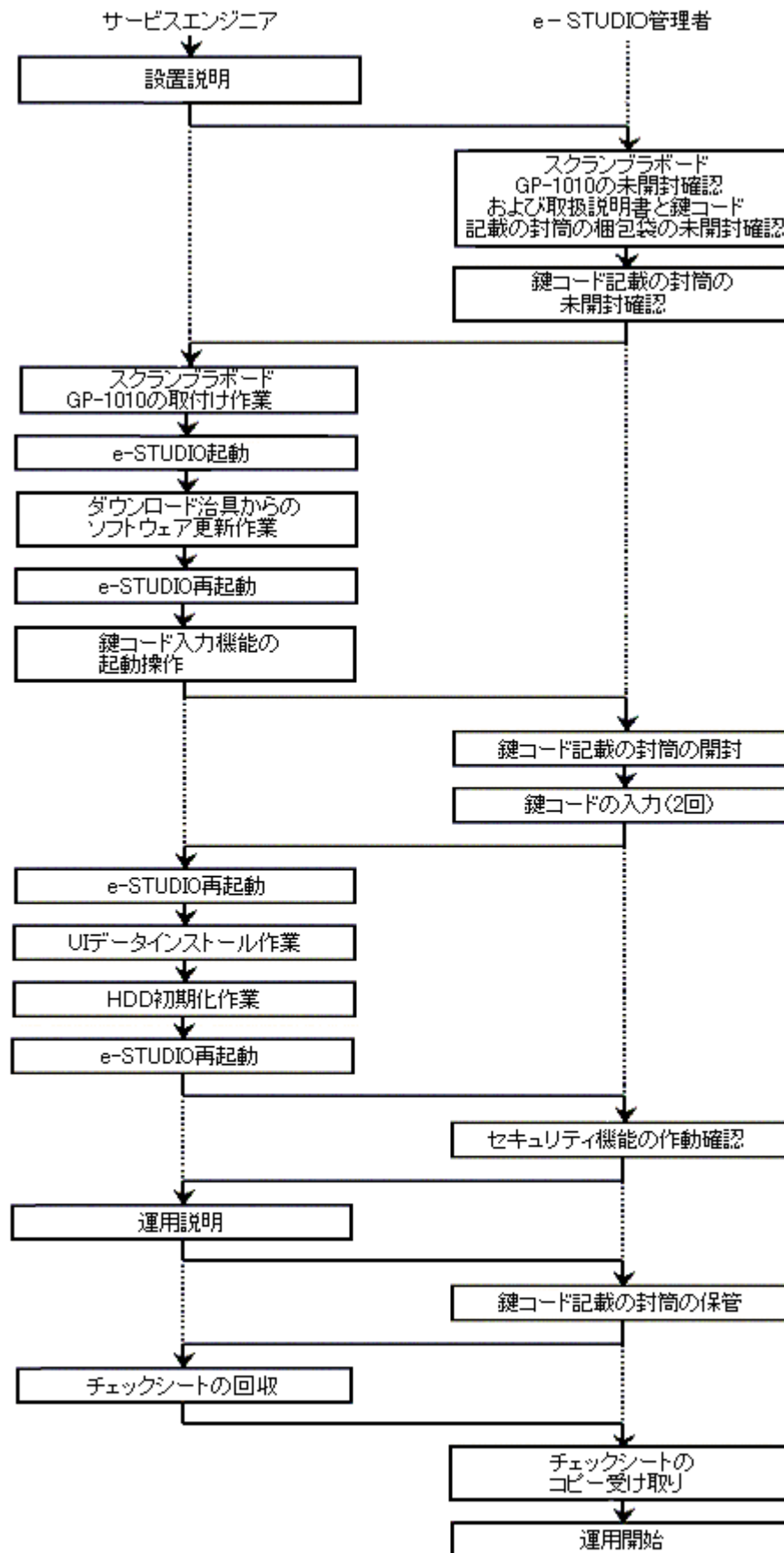
図2.6-1 スクランブラボードGP-1010導入時の作業手順

図2.6-2にe-STUDIO 550/650/810廃棄または交換時の作業手順を示す。
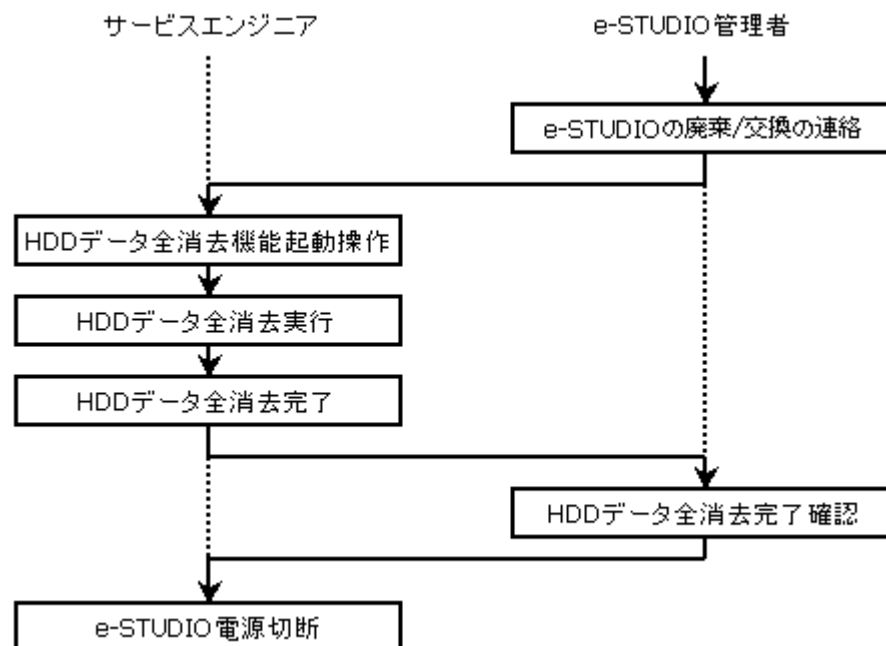
図2.6-2 e-STUDIO 550/650/810廃棄または交換時の作業手順

2.6.4 利用方法

TOEの利用方法の手順を以下に記述する。

・スクランブラボードGP-1010導入時

(1) サービスエンジニアは、e-STUDIO管理者にCheck sheetを渡し、設置のための説明（Check sheetの説明, 鍵コードの保管についての説明, 廃棄または交換時の説明など）を行う。
(2) e-STUDIO管理者は、スクランブラボードが入っている袋のセキュリティシール、及び取扱説明書と鍵コードが記載されている封筒が入っている袋のセキュリティシールが剥されていないことの確認を行い、Check sheetの(1)項にチェックをする。
(3) e-STUDIO管理者は、鍵コードが記載されている封筒の未開封確認を行い、Check sheetの(2)項にチェックをする。
(4) サービスエンジニアは、GP-1010開梱据付指示書に従ってスクランブラボードGP-1010の取付け作業を行う。
(5) サービスエンジニアは、取り付け作業終了後、e-STUDIO 550/650/810の起動を行う。
(6) サービスエンジニアは、ダウンロード治具から、ROMデータのダウンロードを行う。
(7) サービスエンジニアは、ROMデータのダウンロード終了後、e-STUDIO 550/650/810の再起動を行う。
(8) サービスエンジニアは、鍵コード入力画面の表示を行い、e-STUDIO管理者に鍵コードの入力を促す。
(9) e-STUDIO管理者は、鍵コードが記載されている封筒の開封を行う。
(10) e-STUDIO管理者は、サービスエンジニアを含む他の人に鍵コードを見られないように、鍵コード入力を行う。
(11) e-STUDIO管理者は、確認のために二回目の鍵コード入力を行い、Check sheetの(3)項にチェックをする。
(12) サービスエンジニアは、e-STUDIO 550/650/810の再起動を行う。
(13) サービスエンジニアは、UIデータのインストールを行う。
(14) サービスエンジニアは、HDDの初期化を行う。
(15) サービスエンジニアは、e-STUDIO 550/650/810の再起動を行う。
(16) e-STUDIO管理者は、確認ボタンを押下してTOEのバージョンが表示されることの確認を行い、Check sheetの(4)項にチェックをする。（セキュリティ機能の作動確認）
(17) サービスエンジニアは、e-STUDIO管理者に対して運用の説明を行う。
(18) e-STUDIO管理者は、自分以外の人に鍵コードを知られないように、鍵コードが記載されている封筒を厳重に管理し、Check sheetの(5)項にチェックをする。
(19) サービスエンジニアは、Check sheetの回収を行う。
(20) e-STUDIO管理者は、サービスエンジニアからCheck sheetのコピーを受け取る。
(21) e-STUDIO管理者は、運用を開始する。

・通常運用時

(1) 電源の投入により、e-STUDIO 550/650/810の起動処理が開始される。
(2) e-STUDIO利用者は、e-STUDIO 550/650/810の立上げが完了したら、操作パネル上の確認ボタンにより、暗号化機能が正常に動作していることを示すTOEバージョン表示の確認が可能となる。
(3) TOEバージョンの表示が確認できれば、暗号化機能の利用が可能であり、e-STUDIO利用者が紙の文書データを複写、及びファイリングした際に、HDDに格納されるユーザ文書のイメージデータは暗号化される。
(4) e-STUDIO 550/650/810の起動処理中にスクランブラボードの取り外し、またはスクランブラボードの代わりに不正なボード装着の可能性が検出された場合、操作パネル上にサービスマンコール表示されると同時に、全ての機能の利用ができなくなる。その場合、e-STUDIO管理者がその旨をサービスエンジニアに連絡する。

・e-STUDIO 550/650/810廃棄または交換時

(1) e-STUDIO管理者は、サービスエンジニアにe-STUDIO 550/650/810の廃棄または交換の連絡を行う。
(2) サービスエンジニアは、HDDデータ全消去機能を起動する。
(3) サービスエンジニアは、HDDの全データの消去を行う。
(4) サービスエンジニアは、HDDの全データの消去が終了したら、e-STUDIO管理者にHDD全データが消去されたことの確認を促す。
(5) e-STUDIO管理者は、HDD消去状況のパーセンテージ、100%と[Completed]のメッセージが表示されていることで、HDDの全データの消去が終了したことを確認する。
(6) サービスエンジニアは、e-STUDIO 550/650/810の電源を切断する。

3 TOEセキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1 前提条件

前提条件は以下の通りである。

A.KEYCODE_MANAGE

TOEの生成時に入力される鍵コードは、e-STUDIO管理者によって本人以外の人に知られないように管理される。

A.NO_EVIL_ADM

e-STUDIO管理者は、デジタル複写機の運用管理を任された者であり、悪意をもった行為は行わない。

A.NO_EVIL_ENG

サービスエンジニアは、メーカまたはその関連会社、販売会社の正規の社員であり、セキュリティ違反を行なわない。

A.SECURE_KEYCODE

TOEの生成時に入力される鍵コードは、セキュアな値であることが保証された鍵コードであり、e-STUDIO管理者によって正しくTOEにインストールされる。

3.2 脅威

脅威は以下の通りである。

T.HDD_THEFT

e-STUDIO非関係者、または悪意を持ったe-STUDIO利用者が、HDDに不正な解読装置を接続し、ユーザ文書残存データを暴露するかもしれない。

T.SBOARD_REMOVE

e-STUDIO非関係者、または悪意を持ったe-STUDIO利用者が、スクランブラボードを取り外したり、スクランブラボードの代わりに不正なボードを装着することにより、セキュリティ機能が無効化され、ユーザ文書残存データが暴露されるかもしれない。

3.3 組織のセキュリティ方針

組織のセキュリティ方針は以下の通りである。

P.HDD_DISCARD

e-STUDIO 550/650/810本体を廃棄、または交換する時は、サービスエンジニアによってHDDのユーザ文書残存データを全て消去するものとする。

4 セキュリティ対策方針

本章では、TOEセキュリティ対策方針、及び環境のセキュリティ対策方針について記述する。

4.1 TOEセキュリティ対策方針

TOEのセキュリティ対策方針は以下の通りである。

O.HDD_NONEXISTENT

TOEは、HDDにユーザ文書残存データを残さないようにしなければならない。

O.HDD_UNANALYZABLE

TOEは、HDDに不正な解読装置を接続して、ユーザ文書残存データが解読されないようにしなければならない。

O.REMOVE_DETECT

TOEは、TOEの関係者がTOEの利用を開始する前に、システムボードにスクランブラボードが正常に装着されていることを検査しなければならない。
また、セキュリティ機能が正常に動作していることをTOEの関係者が認識できなければならない。
スクランブラボードが取り外されたり、スクランブラボードの代わりに不正なボードが装着されたセキュリティ侵害の場合においては、その事象を検出し、TOEの関係者に通知しなければならない。

4.2 環境のセキュリティ対策方針

運用環境のセキュリティ対策方針は以下の通りである。

OE.HDD_NONEXISTENT

e-STUDIO管理者は、e-STUDIO 550/650/810本体を廃棄または交換する前に、サービスエンジニアへの連絡を行い、TOEにユーザ文書残存データの消去を実施させなければならない。

OE.KEYCODE_MANAGE

e-STUDIO管理者は、TOEの生成時に入力する鍵コードを、本人以外の人に知られないように管理しなければならない。

OE.SECURE_KEYCODE

e-STUDIO管理者は、TOEの生成時に入力する鍵コードを、密封されている封筒に記載されたコード値の通りに入力しなければならない。

OE.TRUST_ADM

e-STUDIO管理者は、利用者部門の責任者が適切な人物を任命しなければならない。

OE.TRUST_ENG

e-STUDIO管理者は、サービスエンジニアが、メーカ、またはその関連会社、販売会社の社員であることを確認しなければなければならない。

IT環境のセキュリティ対策方針は以下の通りである。

OIE.FPT_STM

IT環境は、セキュリティ機能を使用するために、信頼できる時刻を提供しなければならない。

5 ITセキュリティ要件

本章では、TOEセキュリティ要件、及びIT環境のセキュリティ要件について記述する。

5.1 TOEセキュリティ要件

5.1.1 TOEセキュリティ機能要件

TOEセキュリティ機能要件は以下の通りである。

FAU_ARP.1 セキュリティアラーム

下位階層: なし

FAU_ARP.1.1 TSFは、セキュリティ侵害の可能性が検出された場合、[割付: 混乱を最小にするアクションのリスト]を実行しなければならない。

[割付: 混乱を最小にするアクションのリスト]

- サービスマンコール表示
- e-STUDIO利用者機能の受付拒否

依存性: FAU_SAA.1 侵害の可能性の分析

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1 TSFは、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了;

b) 監査の[選択: 最小、基本、詳細、指定なし]レベルのすべての監査対象事象;及び

c) [割付: 上記以外の個別に定義した監査対象事象]。

[選択: 最小、基本、詳細、指定なし]
指定なし

[割付: 上記以外の個別に定義した監査対象事象]

- スクランブラボードの取り外し事象
- スクランブラボード以外の不正なボードの装着事象

FAU_GEN.1.2 TSFは、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗);及び

b) 各監査事象種別に対して、PP/STの機能コンポーネントの監査対象事象の定義に基づいた、[割付: その他の監査関連情報]

[割付: その他の監査関連情報]
なし

依存性: FPT_STM.1 高信頼タイムスタンプ

FAU_SAA.1 侵害の可能性の分析

下位階層: なし

FAU_SAA.1.1 TSFは、監査事象のモニタに規則のセットを適用し、これらの規則に基づきTSP侵害の可能性を示すことができなければならない。

FAU_SAA.1.2

TSFは、監査事象をモニタするための以下の規則を実施しなければならない;

a) セキュリティ侵害の可能性を示すものとして知られている[割付: 定義された監査対象事象のサブセット]をすべて合わせた、あるいは組み合わせたもの;

b) [割付: その他の規則]。

[割付: 定義された監査対象事象のサブセット]

- スクランブラボードの取り外し事象
- スクランブラボード以外の不正なボードの装着事象

[割付: その他の規則]
なし

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.1 監査レビュー

下位階層: なし

FAU_SAR.1.1 TSFは、[割付: 許可利用者]が、[割付: 監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付: 許可利用者]

- TOEの関係者

[割付: 監査情報のリスト]
事象の結果（正常）

FAU_SAR.1.2 TSFは、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性: FAU_GEN.1 監査データ生成

FCS_COP.1 暗号操作

下位階層: なし

FCS_COP.1.1 TSFは、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

[割付: 標準のリスト]
FIPS PUB 46-3

[割付: 暗号アルゴリズム]
Triple DES

[割付: 暗号鍵長]
112bit

[割付: 暗号操作のリスト]

- ユーザ文書データのHDD書込み時の暗号化操作
- ユーザ文書データのHDD読出し時の復号操作

依存性: [FCS_CKM.1 暗号鍵生成
または
FDP_ITC.1 セキュリティ属性なし利用者データのインポート]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FDP_RIP.1 サブセット残存情報保護

下位階層: なし

FDP_RIP.1.1 TSFは、以下のオブジェクト[選択: への資源の割当て、からの資源の割当て解除]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: オブジェクトのリスト]。

[選択: への資源の割当て、からの資源の割当て解除]
からの資源の割当て解除

[割付: オブジェクトのリスト]
ユーザ文書残存データファイル

依存性: なし

FPT_AMT.1 抽象マシンテスト

下位階層: なし

FPT_AMT.1.1 TSFは、TSFの下層にある抽象マシンによって提供されるセキュリティ想定の正しい操作を実証するために、[選択: 初期立ち上げ中、通常操作中に定期的に、許可利用者の要求で、その他の条件]に、テストのスイートを走らせなければならない。

[選択: 初期立ち上げ中、通常操作中に定期的に、許可利用者の要求で、その他の条件]
初期立ち上げ中

依存性: なし

FPT_RVM.1 TSPの非バイパス性

下位階層: なし

FPT_RVM.1.1 TSFは、TSC内の各機能の動作進行が許可される前に、TSP実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

5.1.2 TOEセキュリティ保証要件

TOEセキュリティ保証要件は、EAL2であり、以下の通りである。

- ACM_CAP.2 構成要素
- ADO_DEL.1 配付手続き
- ADO_IGS.1 設置、生成、及び立上げ手順
- ADV_FSP.1 非形式的機能仕様
- ADV_HLD.1 記述的上位レベル設計
- ADV_RCR.1 非形式的対応の実証
- AGD_ADM.1 管理者ガイダンス
- AGD_USR.1 利用者ガイダンス
- ASE_DES.1 セキュリティターゲット、TOE記述、評価要件
- ASE_ENV.1 セキュリティターゲット、セキュリティ環境、評価要件
- ASE_INT.1 セキュリティターゲット、ST概説、評価要件
- ASE_OBJ.1 セキュリティターゲット、セキュリティ対策方針、評価要件
- ASE_PPC.1 セキュリティターゲット、PP主張、評価要件
- ASE_REQ.1 セキュリティターゲット、ITセキュリティ要件、評価要件
- ASE_SRE.1 セキュリティターゲット、明示されたITセキュリティ要件、評価要件
- ASE_TSS.1 セキュリティターゲット、TOE要約仕様、評価要件
- ATE_COV.1 カバレージの証拠
- ATE_FUN.1 機能テスト
- ATE_IND.2 独立テストーサンプル
- AVA_SOF.1 TOEセキュリティ機能強度評価
- AVA_VLA.1 開発者脆弱性分析

5.1.3 最小機能強度宣言

本TOEにおける最小機能強度は、SOF-基本である。確率的または順列的なメカニズムを利用する機能要件はない。FCS_COP.1は、暗号アルゴリズムを利用した機能要件であるため、本最小機能強度宣言の対象としない。

5.2 IT環境のセキュリティ要件

本TOEにおけるIT環境は、e-STUDIO 550/650/810に実装されるシステムボード上のFlash ROMとRTC、及びBSPが対象であり、そのIT環境のセキュリティ要件は以下の通りである。

FPT_STM.1 高信頼タイムスタンプ

下位階層:	なし
FPT_STM.1.1	TSFは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。 **[詳細化]** RTC、及びBSPは、TSF自身の使用のために、高信頼タイムスタンプを提供できなければならない。
依存性:	なし

6 TOE要約仕様

本章では、TOEの要約仕様を記述する。

6.1 TOEセキュリティ機能

表6.1-1に示すように、6.1.1節で説明するTOEセキュリティ機能は、5.1.1節で記述したセキュリティ機能要件を満たすものである。

表6.1-1 TOEセキュリティ機能とセキュリティ機能要件の対応

	FAU_ARP.1	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FCS_COP.1	FDP_RIP.1	FPT_AMT.1	FPT_RVM.1
SF.HDD_ERASE						O		O
SF.REMOVE_DETECT	O		O					O
SF.SBOARD_CHECK		O					O	O
SF.RUN_MESSAGE				O				O
SF.HDD_ENCRYPT					O			O

6.1.1 TOEセキュリティ機能

TOEセキュリティ機能は、以下の通りである。

SF.HDD_ENCRYPT（HDDデータ暗号化／復号）

TOEは、以下の操作に対し、暗号化アルゴリズムとして、Triple DES（FIPS PUB 46-3）、鍵長112bitを使用する。
【暗号化操作】
・ユーザ文書データのHDD書込み時の暗号化操作
・ユーザ文書データのHDD読出し時の復号操作
（FCS_COP.1）
また、TOEは本機能が迂回されないように、スクランブラボード装着時において、システムボードからHDDへのデータ経路と、その逆の経路を単一化し、HDDへの書込み、またはHDDから読出しするデータが必ず暗号化チップを介するようにすることで、HDDへ書込むデータは必ず暗号化チップにより暗号化操作が実施され、HDDから読出されるデータは必ず暗号化チップにより復号操作が実施されるようにする。
（FPT_RVM.1）

SF.HDD_ERASE（HDDデータ全消去）

TOEは、消去実行要求の操作で、以下のデータ値と繰り返し回数により、HDDの実データ領域に書込み(上書き)を行うことによりデータを全消去し、残存情報を保護する。
【データ値】
FF値を暗号化したコード
【繰り返し回数】
1回
（FDP_RIP.1）
また、TOEは本機能が迂回されないように、操作パネル上にHDDの実データ領域の消去開始、及び消去処理中においては、その進捗状況を常に表示・更新することと、消去完了時にその旨を示すメッセージを表示する。
（FPT_RVM.1）

SF.REMOVE_DETECT（暗号化機能迂回検出）

TOEは、以下の監査対象事象のサブセットに示す事象のどれかを検出した場合、セキュリティ侵害と判定する。
【監査対象事象のサブセット】
・スクランブラボードの取り外し事象
・スクランブラボード以外の不正なボード装着事象
（FAU_SAA.1）
TOEは、セキュリティ侵害の判定により、セキュリティ侵害の可能性を検出した場合、以下のアクションを行う。
【アクション】
・操作パネルへのサービスマンコール表示
・e-STUDIO利用者機能の受付拒否によるデジタル複写機の機能停止
（FAU_ARP.1）
また、TOEは本機能が迂回されないように、e-STUDIOの起動処理におけるIDEドライバ初期化処理にて、SF.SBOARD_CHECK実行後にSF.REMOVE_DETECTを実行する手段とし、SF.SBOARD_CHECKによる監査記録が生成されたタイミングで本機能が呼び出されるようにする。
（FPT_RVM.1）

SF.RUN_MESSAGE（暗号化機能動作表示）

TOEは、TOEの関係者に、暗号化機能が適切に動作していることを認識できるように、以下の監査記録情報を読出せるようにする。
【監査記録情報】
・事象の結果（正常）

TOEの関係者に、暗号化機能が適切に動作していることを認識するための情報提供としては、操作パネルからの確認ボタン操作により、事象の結果が正常の場合、TOEバージョンのメッセージデータを生成し、操作パネルにそれを表示する。
（FAU_SAR.1）
また、TOEは本機能が迂回されないように、確認ボタン操作時に実行される複写ユーザインタフェースにおける複写機能の設定情報取得処理の最初に、SF.RUN_MESSAGEの処理を実行する手段とし、操作パネルからの確認ボタン操作のタイミングで、本機能が呼び出されるようにする。
（FPT_RVM.1）

SF.SBOARD_CHECK（暗号化機能実装確認）

TOEは、e-STUDIO 550/650/810の電源投入による初期立ち上げ中に、システムボードにスクランブラボードが正常に装着されていることを確認するために、妥当性テストを実施する。
妥当性のテストでは、次の事象を検知する。
【検知事象】
・システムボードがスクランブラボード上のIDEコントローラチップの識別情報を正しく検知できる。（スクランブラボード正常事象）
・IDEコントローラチップの識別情報を検知できない。（スクランブラボード取り外し事象）
・不正な識別情報を検知した。（スクランブラボード以外の不正なボードの装着事象）
（FPT_AMT.1）

TOEは、スクランブラボードの妥当性テストの結果から、セキュリティ侵害の可能性を検出するため、以下の監査対象事象の監査記録を生成する。TOEは、監査データを記録するのに必要なタイムスタンプ情報を、RTCからIT環境であるOSを介して取得する。
【監査対象事象】
①監査の起動（スクランブラボード正常事象）
②スクランブラボード取り外し事象
③スクランブラボード以外の不正なボードの装着事象

監査の終了が監査対象事象となっていない理由を以下に示す。
デジタル複写機の運用は、一般の計算機と異なり、終了操作によるプロセスやファイルの終了といったシャットダウン処理は存在せず、監査機能を単独で終了させることはできない。監査機能を強制終了させるためには、監査機能プロセスが動作しているOS（VxWorks）にアクセスし、プロセスを終了させることが唯一の方法である。VxWorksにアクセスする方法としては、e-STUDIO本体のシリアルポートから侵入する必要があるが、この方法は悪用不能である。
よって、監査機能の終了は、本体の電源を切断した時にのみ行なわれる。本体電源の切断操作のタイミングで、デジタル複写機の全ての機能は停止してしまうことから、本体電源切断後に、本体、及びTOEに対してアクセスすることは不可能である。
従って、本体の起動（監査の起動）、及び②，③の事象を記録すれば、セキュリティ上の問題は発生しないため、監査の終了を記録する必要はない。
以上の理由から、監査の終了を監査対象事象としない。

また、生成された監査記録には、以下の情報を記録する。
【監査記録情報】
・事象の日付，時刻（RTCから取得したタイムスタンプ）
・事象の種別（スクランブラボードの装着有無）
・サブジェクト識別情報（監査要求元タスク情報）
・事象の結果（正常、またはエラー）
（FAU_GEN.1，FPT_STM.1）

また、TOEは本機能が迂回されないように、e-STUDIOの起動処理におけるIDEドライバ初期化処理の最初に、SF.SBOARD_CHECKを実行する手段とし、e-STUDIOの起動処理が開始され、IDEドライバ初期化処理が開始されたタイミングで、本機能が呼び出されるようにする。
（FPT_RVM.1）

6.1.2 セキュリティメカニズム

本STで参照されているセキュリティメカニズムと、それを使用しているTOEセキュリティ機能の対応は以下の通りである。

表6.1-2 セキュリティメカニズムとTOEセキュリティ機能

セキュリティメカニズム	セキュリティ機能
Triple DES暗号化メカニズム	SF.HDD_ENCRYPT

6.1.3 機能強度主張

TOEセキュリティ機能の内、非暗号で且つ確率的或いは順列的メカニズムに基づくものは、TOEには存在しない。

6.2 保証手段

セキュリティ保証手段として提供される文書、及びTOEに対応するセキュリティ保証要件の対応は以下の通りである。

表6.2-1 セキュリティ保証手段とセキュリティ保証要件

	ACM_CAP.2	ADO_DEL.1	ADO_IGS.1	ADV_FSP.1	ADV_HLD.1	ADV_RCR.1	AGD_ADM.1	AGD_USR.1	ASE_DES.1	ASE_ENV.1	ASE_INT.1	ASE_OBJ.1	ASE_PPC.1	ASE_REQ.1	ASE_SRE.1	ASE_TSS.1	ATE_COV.1	ATE_FUN.1	ATE_IND.2	AVA_SOF.1	AVA_VLA.1
e-STUDIO 550/650/810 SYS-ROM バージョン名付与基準書	O																				
e-STUDIO 550/650/810 CVS管理規約	O																				
サービスドキュメント資料番号発番規定	O																				
製品技術資料(TB)体系規程	O																				
品名コードの発番および変更規程	O																				
e-STUDIO 550/650/810用 HDDエラー要因アクセス機能ファイル構成一覧	O																				
e-STUDIO 550/650/810用 暗号化機能動作確認/鍵コード入力ファイル構成一覧	O																				
e-STUDIO 550/650/810用 暗号化機能迂回検出ファイル構成一覧	O																				
e-STUDIO 550/650/810用 暗号化機能動作表示ファイル構成一覧	O																				
e-STUDIO 550/650/810用 IDEドライバファイル構成一覧	O																				
e-STUDIO 550/650/810用 HDDイレースファイル構成一覧	O																				
PWA-F-DES-340	O																				
スクランブラボード GP-1010 ソフトウェアバージョン管理表	O																				
e-STUDIO 550/650/810 スクランブラボード GP-1010 TOE構成表	O																				
スクランブラボード GP-1010																	O	O	O		
スクランブラボード GP-1010 表現対応分析書						O															
スクランブラボード GP-1010 脆弱性分析書																					O
スクランブラボード GP-1010 機能強度分析書																				O	
スクランブラボード GP-1010 IDEドライバソースコードレビュー記録																	O	O	O		
スクランブラボード GP-1010 例外テスト成績書																	O	O	O		
スクランブラボード GP-1010 例外テスト仕様書																	O	O	O		
スクランブラボード GP-1010 テスト成績書																	O	O	O		
スクランブラボード GP-1010 テスト仕様書																	O	O	O		
スクランブラボード GP-1010 上位レベル設計書(HLD)					O																
スクランブラボード GP-1010 機能仕様書(FSP)				O																	
e-STUDIO 550/650/810用 スクランブラボード GP-1010 Security Target									O	O	O	O	O	O	O	O					

GP-1010 開梱据付指示書		O	O																		
スクランブラボード GP-1010 ROMデータ配付手順書		O																			
スクランブラボード GP-1010 梱包・倉入れ手順書		O																			
スクランブラボード GP-1010 物流手順書		O																			
スクランブラボード GP-1010 構成管理規約	O																				
TOE構成リスト	O																				
Check sheet		O	O																		
e-STUDIO 550/650/810 スクランブラボード GP-1010 取扱説明書		O	O				O	O													
スクランブラボード GP-1010 サービスマニュアル		O	O																		

7 PP主張

PPへの適合は主張しない。

8 根拠

本章では、セキュリティ対策方針、セキュリティ要件、TOE要約仕様、PP主張の根拠について記述する。

8.1 セキュリティ対策方針根拠

8.1.1 セキュリティ対策方針の必要性

以下に、セキュリティ対策方針と前提条件、脅威、組織のセキュリティ方針との対応を示す。表の通り、全てのセキュリティ対策方針は少なくとも一つの前提条件、脅威、組織のセキュリティ方針と対応している。

表8.1-1 セキュリティ対策方針と前提条件、脅威、組織のセキュリティ方針

	A.KEYCODE_MANAGE	A.NO_EVIL_ADM	A.NO_EVIL_ENG	A.SECURE_KEYCODE	P.HDD_DISCARD	T.HDD_THEFT	T.SBOARD_REMOVE
O.HDD_NONEXISTENT					O		
O.HDD_UNANALYZABLE						O	
O.REMOVE_DETECT							O
OE.HDD_NONEXISTENT					O		
OE.KEYCODE_MANAGE	O						
OE.SECURE_KEYCODE				O			
OE.TRUST_ADM		O					
OE.TRUST_ENG			O				
OIE.FPT_STM							O

8.1.2 セキュリティ対策方針の十分性

以下に、セキュリティ対策方針によるTOEセキュリティ環境(前提条件、脅威、組織のセキュリティ方針)の十分性について記述する。

A.KEYCODE_MANAGE

e-STUDIO管理者が、OE.KEYCODE_MANAGEにより、鍵コードを本人以外の人に知られないように管理することによって、e-STUDIO管理者以外への鍵コードの漏えいを防ぐことを実現できる。

A.NO_EVIL_ADM

e-STUDIO管理者は、OE.TRUST_ADMにより、利用部門の責任者が適切な人物を任命することによって、悪意を持った行為を行わないことを実現できる。

A.NO_EVIL_ENG

サービスエンジニアは、製品に関する教育を受けており、製品に関するセキュリティ上の知識を有している。

メーカは、その関連会社、販売会社と守秘義務契約を締結しており、e-STUDIO管理者は、OE.TRUST_ENGにより、サービスエンジニアに対して正規の社員であることを証明させることによって、セキュリティ違反を行なわないことを実現できる。

A.SECURE_KEYCODE

e-STUDIO管理者が、OE.SECURE_KEYCODEにより、密封された封筒に記載されたコード値の通りに鍵コードを入力することによって、セキュアな値であることが保証された鍵コードがTOEにインストールされることを実現できる。

P.HDD_DISCARD

e-STUDIO管理者は、OE.HDD_NONEXISTENTにより、e-STUDIO 550/650/810本体を廃棄、または交換する前に、サービスエンジニアへの連絡を行ない、O.HDD_NONEXISTENTにより、HDDにユーザ文書残存データを残さなくすることにより、e-STUDIO 550/650/810本体を廃棄、または交換する時に、サービスエンジニアによってHDDのユーザ文書残存データを全て消去することを実現できる。

T.HDD_THEFT

T.HDD_THEFTに対抗するためには、HDDから読出した内容を解読できなくすることが必要であり、O.HDD_UNANALYZABLEにて、HDDに保存されているデータが読出せた場合でもその内容を解読できなくすることにより対抗できる。

T.SBOARD_REMOVE

T.SBOARD_REMOVEに対抗するためには、セキュリティ機能が正常に動作しているのか、または無効な状態なのかを認識する必要があり、O.REMOVE_DETECTにてセキュリティ機能が正常に動作している場合は、その状態をTOEの関係者に認識させることと、スクランブラボードを取り外したり、スクランブラボードの代わりに不正なボードを装着することによるセキュリティ侵害の場合は、その事象を検出し、TOEの関係者に通知することにより対抗できる。

尚、OIE.FPT_STMは、O.REMOVE_DETECTを実現するのに必要なTOEセキュリティ機能要件の依存性をIT環境のセキュリティ要件により実現することで、本脅威に関係づけるものである。

8.2 セキュリティ要件根拠

8.2.1 セキュリティ機能要件の必要性

以下に、セキュリティ機能要件とセキュリティ対策方針との対応を示す。
表の通り、全てのTOEセキュリティ機能要件は少なくとも一つのTOEのセキュリティ対策方針と対応している。

表8.2-1 TOEセキュリティ機能要件とTOEのセキュリティ対策方針

	O.HDD_NONEXISTENT	O.HDD_UNANALYZABLE	O.REMOVE_DETECT	OIE.FPT_STM
FAU_ARP.1			O	
FAU_GEN.1			O	
FAU_SAA.1			O	
FAU_SAR.1			O	
FCS_COP.1		O		
FDP_RIP.1	O			
FPT_AMT.1			O	
FPT_RVM.1	−	−	−	
FPT_STM.1			−	O

(注: 'O'は対策方針と直接対応している事を、'−'は機能要件の依存性、或いは相互サポートの対応を辿って関係している事を示す。)

8.2.2 セキュリティ機能要件の十分性

以下に、セキュリティ機能要件によるセキュリティ対策方針の十分性を記述する。

O.HDD_NONEXISTENT

FDP_RIP.1によって、HDDの以前の情報の内容を利用できなくすることで、ユーザ文書残存データを残さないというセキュリティ対策方針を実現できる。

O.HDD_UNANALYZABLE

FCS_COP.1によって、FIPS PUB 46-3に基づき暗号化することで、ユーザ文書残存データが解読されないようにするというセキュリティ対策方針を実現できる。

O.REMOVE_DETECT

①FPT_AMT.1によって、e-STUDIO 550/650/810初期立ち上げ中に、システムボードにスクランブラボードが正常に装着されていることを検知するかどうかのテストを実行する。
②FAU_GEN.1によって、セキュリティ機能が正常に動作していることを確認するためと、セキュリティ侵害を検出するための監査データを生成する。
③FAU_SAA.1によって、FAU_GEN.1で生成された監査データから、スクランブラボードが取り外されたり、スクランブラボードの代わりに不正なボードが装着されたセキュリティ侵害を検出するための分析を行う。
④FAU_ARP.1によって、FAU_SAA.1の分析の結果、セキュリティ侵害の可能性が検出された場合、サービスマンコール表示を行うことにより、TOEの関係者に通知する。
⑤FAU_SAR.1によって、FAU_GEN.1で生成された監査データの事象の結果が正常の場合、TOEのバージョンを表示する。
①により、TOEの関係者がTOEの利用開始前にセキュリティ機能が正常に動作していることを確認するという対策方針を実現できる。
②, ③, ④により、スクランブラボードが取り外されたり、スクランブラボードの代わりに、不正なボードが装着されたセキュリティ侵害を検出し、TOEの関係者に通知するという対策方針を実現できる。
⑤により、セキュリティ機能が正常に動作していることを、TOEの関係者に認識させるという対策方針を実現できる。

OIE.FPT_STM

FPT_STM.1により、内部時計が実時間に準じた時間データを発生させることで、セキュリティ機能を使用するために、信頼できる時刻を提供するというIT環境の対策方針を実現できる。

8.2.3 セキュリティ機能要件の依存性の根拠

以下に、セキュリティ機能要件の依存性の根拠を記述する。

FAU_ARP.1

FAU_SAA.1により、依存性は満たされている。

FAU_GEN.1

FPT_STM.1により、依存性は満たされている。

FAU_SAA.1

FAU_GEN.1により、依存性は満たされている。

FAU_SAR.1

FAU_GEN.1により、依存性は満たされている。

FCS_COP.1

FCS_COP.1の依存関係は満たされていないが、問題がない根拠を以下に示す。
①暗号鍵はTOE外の暗号鍵作成会社で作成され、鍵コードとして提供される。e-STUDIO管理者は、鍵コードをTOEインストール時に一度だけ入力し、システムボード上の拡張NVRAMに暗号鍵データとしてインポートされる。その後の暗号化、復号操作においては、インポートされた暗号鍵データを継続して使用するため、TOEにおいて暗号鍵を生成する必要と、暗号鍵を破棄する必要はない。
②暗号鍵のインポートは、TOEインストール時に行われることから、TOE利用時におけるTSC外からのインポートの必要はない。
③暗号鍵は、暗号鍵作成会社より提供されるもので、FIPS140-2の統計的乱数性の検定に適合したセキュアであることが保証された暗号鍵である。暗号鍵のセキュリティ属性は、暗号鍵長のみである。暗号鍵は指定の暗号鍵長で生成され、その暗号鍵がインポートされる。セキュアであることが保証された暗号鍵がインポートされ、その暗号鍵が継続して使用されることから、セキュリティ属性としてセキュアな値だけが受け入れられることを保証する必要はない。
①により、FCS_CKM.1, FCS_CKM.4の依存関係は不要である。②により、FDP_ITC.1の依存関係は不要である。③により、FMT_MSA.2の依存関係は不要である。

FDP_RIP.1

満たすべき依存性は存在しない。

FPT_AMT.1

満たすべき依存性は存在しない。

FPT_RVM.1

満たすべき依存性は存在しない。

FPT_STM.1

満たすべき依存性は存在しない。

8.2.4 セキュリティ要件の相互作用

以下に、機能要件とその機能要件をサポートする要件の対応を示す。

表8.2-2 機能要件と相互サポート対応

機能要件	相互サポート要件
FAU_ARP.1	FPT_RVM.1
FAU_GEN.1	FPT_RVM.1
FAU_SAA.1	FPT_RVM.1
FAU_SAR.1	FPT_RVM.1
FCS_COP.1	FPT_RVM.1
FDP_RIP.1	FPT_RVM.1
FPT_AMT.1	FPT_RVM.1
FPT_RVM.1	なし

FPT_RVM.1＜迂回防止＞

①「e-STUDIO 550/650/810」の起動処理において、デジタル複写機の機能が実行される前のIDEドライバ初期化処理にて、暗号化機能実装確認（FPT_AMT.1, FAU_GEN.1）, 暗号化機能迂回検出（FAU_SAA.1, FAU_ARP.1）の順に必ず呼び出され、成功することが保証される。
②TOEの関係者による操作パネルからの確認操作時に、複写ユーザインタフェースにおける複写機能の設定情報取得処理の初めに、暗号化機能動作確認でスクランブラボードの装着有無情報をNVRAMから取得し、その後、暗号化機能動作表示機能（FAU_SAR.1）は必ず呼び出され、成功することが保証される。
③サービスエンジニアによるHDDデータ全消去機能の実行要求時に、HDDの実データ領域の消去処理中に、その進捗状況を操作パネル上に常に表示・更新することと、消去完了時にその旨を示すメッセージを表示することにより、HDDデータ全消去（FDP_RIP.1）は迂回されないことが保証される。
④「e-STUDIO 550/650/810」に、スクランブラボードが正常に装着されている状態で、HDDへの書込みの時のシステムボードからHDDへのデータ経路と、HDDからの呼び出し時のその逆の経路は単一化されており、データは必ず暗号化チップを介することにより、HDDデータ暗号化／復号（FCS_COP.1）の機能は必ず呼び出され、成功することが保証される。
以上、FPT_RVM.1により、デジタル複写機の各種機能が実行される前に必ず対象のセキュリティ機能が呼び出され、成功することが保証されることにより迂回されない。

本TOEでは、許可利用者といったTOEを操作するために必要な権利や特権を有するTSFはない。TOEには、外部からの利用者を代行して働くサブジェクトは存在せず、TSFの他の利用者のデータにアクセスする利用者について関知する必要がないため、アクセス制御や情報フロー制御を実施しない。 よって本TOEでは、信頼できないサブジェクトによる外部の干渉、及び改ざんからTSFを保護する必要が無いため、相互サポートにおけるFPT_SEP.1の要件は不要である。

8.2.5 最小機能強度の妥当性

本TOEは、ネットワークに接続されない環境で使用される製品であり、TOEへの想定される攻撃は、保護資産の不正な解読やTOEの取り外し、及び置き換えなどの直接的な不正行為に制限される。TOEが設置されている一般のオフィス環境において、TOEに直接的に不正行為を行う攻撃者は、高度な情報処理技術を持たない低レベルの攻撃力である。
従って、低レベルの攻撃力に対抗するための最小機能強度は、SOF-基本で満足できる。

8.2.6 評価保証レベルの妥当性

評価保証レベルは、EAL2である。

本TOEは、一般のオフィス等で使用される商業的製品であるデジタル複写機に実装されるものである。本TOEの想定するデジタル複写機が運用される環境は、電話回線やネットワークなどへの接続はなく、独立している。運用環境の制約から、デジタル複写機へのアクセスは、e-STUDIO関係者と物理的にアクセス可能なe-STUDIO非関係者に制限される。e-STUDIO非関係者の攻撃能力は低レベルであり、保護資産に対する攻撃の種別は限られていることから、その可能性は低い。
以上により、コストに見合うセキュリティ侵害に対抗できればよい。

従って、評価保証レベル2の保証パッケージが妥当である。

8.2.7 セキュリティ保証要件の根拠

以下のセキュリティ保証要件は、評価保証レベル2を満たす為に必要である。

- ACM_CAP.2 構成要素
- ADO_DEL.1 配付手続き
- ADO_IGS.1 設置、生成、及び立上げ手順
- ADV_FSP.1 非形式的機能仕様
- ADV_HLD.1 記述的上位レベル設計
- ADV_RCR.1 非形式的対応の実証
- AGD_ADM.1 管理者ガイダンス
- AGD_USR.1 利用者ガイダンス
- ATE_COV.1 カバレージの証拠
- ATE_FUN.1 機能テスト
- ATE_IND.2 独立テスト−サンプル
- AVA_SOF.1 TOEセキュリティ機能強度評価
- AVA_VLA.1 開発者脆弱性分析

また、以下のセキュリティ保証要件は、セキュリティターゲット評価に必要である。

- ASE_DES.1 セキュリティターゲット、TOE記述、評価要件
- ASE_ENV.1 セキュリティターゲット、セキュリティ環境、評価要件
- ASE_INT.1 セキュリティターゲット、ST概説、評価要件
- ASE_OBJ.1 セキュリティターゲット、セキュリティ対策方針、評価要件
- ASE_PPC.1 セキュリティターゲット、PP主張、評価要件
- ASE_REQ.1 セキュリティターゲット、ITセキュリティ要件、評価要件
- ASE_SRE.1 セキュリティターゲット、明示されたITセキュリティ要件、評価要件
- ASE_TSS.1 セキュリティターゲット、TOE要約仕様、評価要件

8.2.8 セキュリティ保証要件の依存性の根拠

EAL2適合により依存性を満たしている。
以下に、セキュリティ保証要件毎の依存性の根拠を記述する。

ACM_CAP.2
満たすべき依存性は存在しない

ADO_DEL.1
満たすべき依存性は存在しない

ADO_IGS.1
AGD_ADM.1により、依存性は満たされている。

ADV_FSP.1
ADV_RCR.1により、依存性は満たされている。

ADV_HLD.1
ADV_FSP.1、ADV_RCR.1により、依存性は満たされている。

ADV_RCR.1
満たすべき依存性は存在しない

AGD_ADM.1
ADV_FSP.1により、依存性は満たされている。

AGD_USR.1
ADV_FSP.1により、依存性は満たされている。

ASE_DES.1
ASE_ENV.1、ASE_INT.1、ASE_OBJ.1、ASE_PPC.1、ASE_REQ.1、ASE_TSS.1により、依存性は満たされている。

ASE_ENV.1
満たすべき依存性は存在しない

ASE_INT.1
ASE_DES.1、ASE_ENV.1、ASE_OBJ.1、ASE_PPC.1、ASE_REQ.1、ASE_TSS.1により、依存性は満たされている。

ASE_OBJ.1
ASE_ENV.1により、依存性は満たされている。

ASE_PPC.1
ASE_OBJ.1、ASE_REQ.1により、依存性は満たされている。

ASE_REQ.1
ASE_OBJ.1により、依存性は満たされている。

ASE_SRE.1
ASE_REQ.1により、依存性は満たされている。

ASE_TSS.1
ASE_REQ.1により、依存性は満たされている。

ATE_COV.1
ADV_FSP.1、ATE_FUN.1により、依存性は満たされている。

ATE_FUN.1
満たすべき依存性は存在しない

ATE_IND.2
ADV_FSP.1、AGD_ADM.1、AGD_USR.1により、依存性は満たされている。

AVA_SOF.1
ADV_FSP.1、ADV_HLD.1により、依存性は満たされている。

AVA_VLA.1
ADV_FSP.1、AGD_ADM.1、AGD_USR.1、ADV_HLD.1により、依存性は満たされている。

8.3 TOE要約仕様根拠

8.3.1 セキュリティ機能の必要性

以下にTOEセキュリティ機能とセキュリティ機能要件との対応を示す。
表の通り、全てのTOEセキュリティ機能は少なくとも一つのTOEセキュリティ機能要件と対応している。

表8.3-1 TOEセキュリティ機能とセキュリティ機能要件

	FAU_ARP.1	FAU_GEN.1	FAU_SAA.1	FAU_SAR.1	FCS_COP.1	FDP_RIP.1	FPT_AMT.1	FPT_RVM.1
SF.HDD_ERASE						O		O
SF.REMOVE_DETECT	O		O					O
SF.SBOARD_CHECK		O					O	O
SF.RUN_MESSAGE				O				O
SF.HDD_ENCRYPT					O			O

8.3.2 セキュリティ機能の十分性

以下に、セキュリティ機能によるセキュリティ機能要件の十分性を記述する。

FAU_ARP.1

SF.REMOVE_DETECTにより、セキュリティ侵害の可能性を検出した場合、操作パネル上にサービスエンジニアを呼び出す旨のサービスマンコール表示と、e-STUDIO利用者機能の受付拒否により機能の使用を停止させる。

以上により、SF.REMOVE_DETECTでのセキュリティアラームは保証できる。

FAU_GEN.1

SF.SBOARD_CHECKにより、IDEコントローラチップの識別情報から監査データの生成を行う。監査データには、事象の日付，時刻（RTCから取得したタイムスタンプ）と、事象の種別（スクランブラボードの装着有無），サブジェクト識別情報（監査要求元タスク情報），事象の結果（正常、またはエラー）を記録する。

以上により、SF.SBOARD_CHECKでの監査データ生成は保証できる。

FAU_SAA.1

SF.REMOVE_DETECTにより、定義されたセキュリティ侵害の判定基準に基づき、監査データの判定を行う。

以上により、SF.REMOVE_DETECTでの侵害の可能性の分析は保証できる。

FAU_SAR.1

SF.RUN_MESSAGEにより、TOEの関係者に暗号化機能が適切に動作していることを認識するため、操作パネルからの確認要求時に、TOEのバージョン表示を行う。

以上により、SF.RUN_MESSAGEでの監査レビューは保証できる。

尚、鑑査記録をTOEの関係者に提供することについて、鑑査記録は秘密情報でないことから問題は無い。

FCS_COP.1

SF.HDD_ENCRYPTにより、定義された暗号操作に合致する特定された暗号アルゴリズムと、指定された暗号鍵長に従って暗号操作を行う。

以上により、SF.HDD_ENCRYPTでの暗号操作は保証できる。

FDP_RIP.1

SF.HDD_ERASEにより、e-STUDIO 550/650/810廃棄または交換時にサービスエンジニアによって、HDDの実データ領域の残存情報を消去する。

以上により、SF.HDD_ERASEでのサブセット残存情報保護は保証できる。

FPT_AMT.1

SF.SBOARD_CHECKにより、e-STUDIO 550/650/810の電源投入による初期立ち上げ中に、システムボードにスクランブラボードが正常に装着されていることを確認するために、妥当性テストを実行する。

以上により、SF.SBOARD_CHECKでの抽象マシンテストは保証できる。

FPT_RVM.1

①SF.HDD_ENCRYPTにより、スクランブラボード装着時に、システムボードからHDDへのデータ経路と、その逆の経路を単一化し、HDDへの書込み、またはHDDから読出されるデータは、必ず暗号化チップを介するようにする。

②SF.SBOARD_CHECKにより、e-STUDIO 550/650/810の起動処理が開始され、IDEドライバ初期化処理が開始されるタイミングで、スクランブラボードGP-1010の装着確認を行い、監査記録を生成する。

③SF.REMOVE_DETECTにより、SF.SBOAD_CHECKによる監査記録が生成されたタイミングで、セキュリティ侵害の判定を行い、セキュリティ侵害と判定された場合、サービスマンコール表示と、e-STUDIO利用者機能の受付拒否によるデジタル複写機の機能停止

を行なう。
④SF.RUN_MESSAGEにより、ボード確認結果が正常な場合、確認ボタン操作時に実行される複写ユーザインタフェースにおける複写機能の設定情報取得処理の最初に、TOEバージョンのメッセージデータを生成して、操作パネルに表示する。
⑤SF.HDD_ERASEにより、HDDの実データ領域の消去開始、および消去処理中に、HDDの全データ領域の消去処理の進捗状況を常に操作パネル上に表示・更新し、消去完了時にその旨を示すメッセージを表示する。
①により、SF.HDD_ENCRYPTでのTSPの非バイパス性は保証できる。
②により、SF.SBOARD_CHECK，③により、SF.REMOVE_DETECT，④により、SF.RUN_MESSAGEでのTSPの非バイパス性は保証できる。
⑤により、SF.HDD_ERASEでのTSPの非バイパス性は保証できる。

8.3.3 機能強度の根拠

本TOEにおいて、根拠を示すべき、確率的或いは順列的メカニズムを持つセキュリティ機能は存在しない。

8.3.4 保証手段の根拠

セキュリティ保証手段が、保証要件を満たすのに適切な根拠を記述する。
全てのEAL2のセキュリティ保証要件は、セキュリティ保証手段となるドキュメント、及びTOEに対応付けられている。また、当該ドキュメント、及びTOEによって、セキュリティ保証要件が要求する証拠は網羅されている。表8.3-2に、各保証手段毎の内容を示す。

表8.3-2 セキュリティ保証手段一覧

ドキュメント／TOE名称	内容	保証要件クラス	保証要件コンポーネント
e-STUDIO 550/650/810 スクランブラボード GP-1010 TOE構成表	TOEの構成表。 TOEの構成するバージョン、及び識別子が記述されている。	ACM 構成管理	ACM_CAP.2
スクランブラボード GP-1010 ソフトウェアバージョン管理表	TOE部分のソフトウェアバージョン管理表。 TOE部分のソフトウェアのバージョン管理と、オブジェクトコードをまとめた管理表が記述されている。		
PWA-F-DES-340	スクランブラボードの図面。 TOEであるスクランブラボードに実装されている部品構成や変更履歴が記述されている。		
e-STUDIO 550/650/810用 HDDイレースファイル構成一覧	HDDのイレースファイル構成一覧。 e-STUDIO550/650/810用システムソフトウェアバージョンと、HDDイレース機能を構成するファイル一覧が記述されている。		
e-STUDIO 550/650/810用 IDEドライバファイル構成一覧	IDEドライバのファイル構成一覧。 e-STUDIO550/650/810用システムソフトウェアバージョンと、IDEドライバを構成するファイル一覧が記述されている。		
e-STUDIO 550/650/810用 暗号化機能動作表示ファイル構成一覧	暗号化機能の動作表示ファイル構成一覧。 e-STUDIO550/650/810用システムソフトウェアバージョンと、暗号化機能動作表示を構成するファイル一覧が記述されている。		
e-STUDIO 550/650/810用 暗号化機能迂回検出ファイル構成一覧	暗号化機能の迂回検出ファイル構成一覧。 e-STUDIO550/650/810用システムソフトウェアバージョンと、暗号化機能迂回検出を構成するファイル一覧が記述されている。		
e-STUDIO 550/650/810用 暗号化機能動作確認/鍵コード入力ファイル構成一覧	暗号化機能の動作確認、及び鍵コード入力ファイル一覧。 e-STUDIO550/650/810用システムソフトウェアバージョンと、暗号化機能動作確認／鍵コード入力を構成するファイル一覧が記述されている。		
e-STUDIO 550/650/810用 エラー要因アクセス機能ファイル構成一覧	HDDのエラー要因アクセス機能ファイル一覧。 e-STUDIO550/650/810用システムソフトウェアバージョンと、HDDエラー要因アクセス機能を構成するファイル一覧が記述されている。		
TOE構成リスト	TOEの構成要素リスト。 TOEを構成するハードウェア，ソフトウェア，ドキュメントを一意に識別するための情報が記述されている。		
スクランブラボード GP-1010 構成管理規約	TOEの構成管理の対象とその管理方法を定めた規約。 TOEの開発に関連するドキュメント，ソースコード、及びオブジェクトコードなどを対象とした構成管理方法が記述されている。		
	図面の発番規定。		

品名コードの発番および変更規程	図面等の品名コードの発番と、設計変更についての規程が記述されている。		
製品技術資料(TB)体系規程	製品技術資料の体系及び発番規定。 製品技術資料及びセキュリティ保証手段ドキュメント等の発番、分類及びファイリング，保管についての規程が記述されている。		
サービスドキュメント資料番号発番規定	ガイダンス関係の発番規定。 取扱説明書等ガイダンスの発番と、変更についての規定が記述されている。		
e-STUDIO 550/650/810 CVS管理規約	ソフトウェアのCVS登録管理規約。 ソフトウェア開発の際に必要なネーミング，バージョン管理及びCVS登録ルールが記述されている。		
e-STUDIO 550/650/810 SYS-ROM バージョン名付与基準書	SYS-ROMのバージョン名付与規定。 ROMデータが書込みされたEPROMのバージョン名の付与基準が記述されている。		
スクランブラボード GP-1010 サービスマニュアル	サービスエンジニア向けガイダンス文書。 サービスエンジニアに対するTOEの設置手順、及びトラブルシューティング手順が記述されている。TOEの設置に関し、e-STUDIO管理者と実施するTOEの装着及び立上げ作業における注意事項、TOEのソフトウェアインストール手順が詳述されている。また、TOEを含むデジタル複写機の廃棄(交換)時における、HDDの消去手順も記述されている。	ADO 配付と運用 AGD ガイダンス文書	ADO_DEL.1 ADO_IGS.1
e-STUDIO 550/650/810 スクランブラボード GP-1010 取扱説明書	e-STUDIO管理者とe-STUDIO利用者向けガイダンス文書。 e-STUDIO利用者向けに、TOEの機能説明、及びTSFの作動確認方法、e-STUDIO管理者向けに、鍵コードの入力や管理方法の説明や残存データ全消去の確認方法が記述されている。		ADO_DEL.1 ADO_IGS.1 AGD_ADM.1 AGD_USR.1
Check sheet	TOEの配付手続きに関する証拠資料。 TOEが配送途中で改変されていないことをe-STUDIO管理者がチェックするためのシートであり、TOEの梱包状態、鍵コード封筒の状態、TSFの作動などの確認を行うための項目が記述されている。		ADO_DEL.1 ADO_IGS.1
スクランブラボード GP-1010 物流手順書	TOEの配付手続きに関する証拠資料。 TOEのハードウェアとドキュメントを対象に、メーカの倉庫からの倉出しから客先据付までの管理と配送設備、手続きについて記述されている。		ADO_DEL.1
スクランブラボード GP-1010 梱包・倉入れ手順書	TOEの配付手続きに関する証拠資料。 TOEのハードウェアとドキュメントを対象に、梱包からメーカ倉庫への倉入れまでの管理と配送設備、手続きについて記述されている。		ADO_DEL.1
スクランブラボード GP-1010 ROMデータ配付手順書	TOEの配付手続きに関する証拠資料。 TOEのソフトウェアであるROMデータをe-STUDIO 550/650/810のシステムボードのFlash ROMにダウンロードするまでの管理と配送設備、手続きについて記述されている。		ADO_DEL.1
GP-1010 開梱据付指示書	TOEの設置から立上げまでの手順書。 サービスエンジニアが行う、TOEの設置から立上げまでの手順が記述されている。		ADO_DEL.1 ADO_IGS.1
スクランブラボード GP-1010 機能仕様書(FSP)	機能仕様書。 TSFのふるまいとTSFインタフェース、TSF以外の機能についての外部インタフェースについて記述されている。	ADV 開発	ADV_FSP.1
スクランブラボード GP-1010 上位レベル設計書(HLD)	上位レベル設計書。 サブシステムの観点からTSFを記述したものであり、TSFの構造、サブシステムのインタフェースについて記述されている。		ADV_HLD.1
スクランブラボード GP-1010 表現対応分析書	表現対応分析書。 STにおける要約仕様のセキュリティ機能と機能仕様書におけるセキュリティ機能の関係、機能仕様書におけるセキュリティ機能と上位レベル設計書におけるサブシステムの関係について分析した結果について記述されている。		ADV_RCR.1
			ASE_DES.1 ASE_ENV.1

e-STUDIO 550/650/810用 スクランブラボード GP-1010 Security Target	セキュリティターゲット。	ASE セキュリティターゲット評価	ASE_INT.1 ASE_OBJ.1 ASE_PPC.1 ASE_REQ.1 ASE_SRE.1 ASE_TSS.1
スクランブラボード GP-1010 テスト仕様書	テスト証拠資料。 TSFが仕様通りに実行されることを実証するための機能テスト項目、テスト手順、期待されるテスト結果について記述されている。	ATE テスト	ATE_COV.1 ATE_FUN.1 ATE_IND.2
スクランブラボード GP-1010 テスト成績書	テスト証拠資料。 テスト仕様書に基づいて、TSFがその機能仕様に対応してテストを行った結果について記述されている。		
スクランブラボード GP-1010 例外テスト仕様書	テスト証拠資料。 テスト仕様書に記述されている機能テスト項目の中で、TOEの変更なしではテストできない例外的なテスト項目に対して、テスト手順、期待されるテスト結果について記述されている。		
スクランブラボード GP-1010 例外テスト成績書	テスト証拠資料。 例外テスト仕様書に基づいて、機能テストを行った結果について記述されている。		
スクランブラボード GP-1010 IDEドライバソースコードレビュー記録	テスト証拠資料。 テスト仕様書に記述されている機能テスト項目の中で、テストでは再現できない異常動作に関し、IDEドライバのソースコード上から異常発生時の動作を検証しセキュリティ機能上問題のないことを確認したレビュー記録である。		
スクランブラボード GP-1010	TOE。		
スクランブラボード GP-1010 機能強度分析書	機能強度分析書。 TOE における暗号化メカニズムを除く、確率的または順列的セキュリティメカニズムを有するセキュリティ機能に対して、機能強度分析を実施した結果について記述されている。但し、本TOEでは機能強度分析対象となる確率的または順列的セキュリティメカニズムを有するセキュリティ機能は存在しない。	AVA 脆弱性評定	AVA_SOF.1
スクランブラボード GP-1010 脆弱性分析書	脆弱性分析書。 明らかなセキュリティ脆弱性の存在を探索し、TOE の意図する環境において、それらの脆弱性が悪用され得ないことを確認する脆弱性分析を実施した結果について記述されている。		AVA_VLA.1

8.4 PP主張根拠

本STにて適合するPPはない。